



**Baker
McKenzie.**

Looking Ahead

TECHNOLOGY, MEDIA & TELECOMMUNICATIONS

2019

In this issue...

Foreword	03
<hr/>	
[1] Legislators and regulators are responding to digital business models	04
Antitrust compliance tips for companies in a digital world	05
Taxation of the digital economy	08
Tech companies, ethics and human rights	10
The modern workforce	12
Content governance obligations for online intermediary platforms	15
<hr/>	
[2] Data is king but compliance is key	18
Data monetization – shifting tides	19
Personal data regulation – trend spotting	21
Global data center trends	24
<hr/>	
[3] Looking at China	26
The growing influence of Chinese tech companies	26
<hr/>	
[4] Trade wars to unfold and supply chains to change	29
Trade wars and their impact on supply chains and sales	30
Moving towards a closed-loop supply chain	31
<hr/>	
[5] Regulating telecoms, ISPs, OTT and beyond	32
5G roll-out and EU Electronic Communications Code	33
Access to data – a new era for national security and law enforcement	35
Net neutrality – where are we heading?	38
<hr/>	
[6] The transactional landscape	40
Deal activity in TMT	41
Content media: the transactional landscape	43
<hr/>	
[7] The benefits and challenges of living in an interconnected world	45
Autonomous vehicles — where are we driving to?	46
The growing importance of standard essential patents in times of digitalization	49

Foreword



Raffaele Giarda
Chair, Global TMT

Dear readers,

What does 2019 hold for businesses in the Technology, Media and Telecommunications sector and what legal and regulatory trends should be on their radar? A complex question in a world in which the boundaries between areas are blurring to an extent that car manufacturers are becoming tech companies, traditional content producers are launching their own direct-to-consumer streaming services, and telecommunications providers are moving into adjacent industries to make up for declines in traditional revenues. Everywhere, conventional business models are under increased pressure for change and no player seems to be immune from disruptive technologies.

Governments, policy makers and regulators are equally struggling to grapple with the speed at which technology pervades every aspect of society. They are looking at elaborating new rules that foster socially beneficial innovation, preserve human values and nurture competition.

Big tech is at the center of all such debates, as most recently evidenced at the World Economic Forum in Davos where significant attention was dedicated to topics such as data governance, digital ethics and how to craft rules governing e-commerce and cross-border data flows fit for global trade. There is a real sense of urgency. 2019 will not bring all the answers to the complex questions we face, but we are at a turning point and the direction of travel should become clearer in many respects.

Our global TMT team, consisting of over 1500 lawyers in 78 offices, covering all practices of law, is pleased to bring you a selection of trends and developments to watch in 2019. We have grouped these into seven themes.

Enjoy the read and feel free to get in touch with any of the authors or myself.

Legislators and regulators are responding to digital business models

Around the world, lawmakers and regulators from many disciplines are responding to digital business models. **Antitrust agencies** have their eyes set on the tech sector and we expect a continued focus on platforms, the data advantage and attempts of making antitrust rules and procedures fit for the digital age. As the **modern workforce and the gig economy** continue their exponential growth, across jurisdictions pressure is building on governments to reform employment laws to provide adequate protection and rights for both workers and employers. **In the world of tax**, 2018 has been dominated by discussions and proposals aimed at making tax rules fit for the digital economy. This has brought significant uncertainty and tech firms must brace themselves for major change in the form of new tax rules being crafted and implemented in 2019 and beyond. Rapid advances in powerful tools promise a world more intertwined with technology than ever. This raises issues of **ethics, human rights and accountability**, and responsibility for preserving values is increasingly shifted onto tech companies. Finally, the **fight against illegal online content** goes on and while the EU will continue to drive its controversial copyright reform, other countries are also looking to revise the content governance obligations for online intermediary platforms.

Antitrust compliance tips for companies in a digital world

By challenging older business models, ramping up the pressure and giving consumers more choice at lower prices, tech companies do precisely what antitrust law and policy seeks to achieve.

But the rapid growth, strength and influence of tech companies — despite their notable advancements with respect to nearly every corner of the economy — is a mounting concern for some antitrust agencies. This is especially the case in Europe where high profile investigations and speeches have focused on the role of platforms, the importance of data, and conduct that is argued to have excluded competitors.

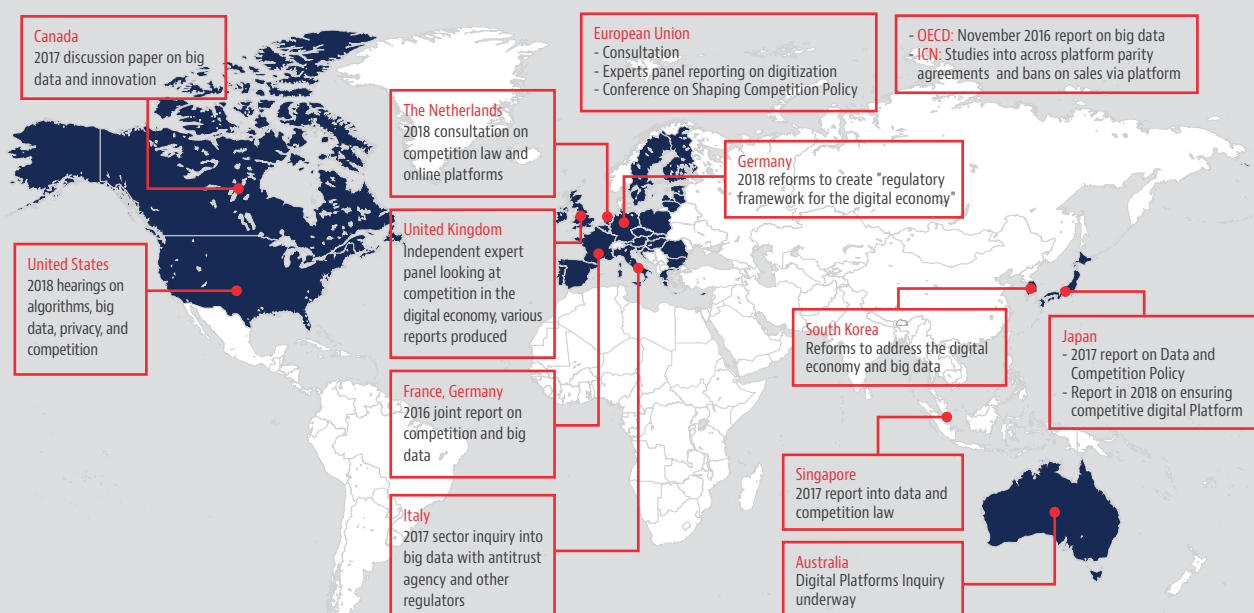
Antitrust clearly has a role to play in ensuring that markets stay open and, because digitalization now touches all sectors of the economy, the antitrust agencies are feeling the weight of the responsibility to get the analysis right. With that weight comes significant responsibility, as over-enforcement or market "tinkering"

with respect to any industry — but particularly technology — risks doing significant harm and frustrating the purpose of their missions.

It is not always straightforward. Case-by-case evaluations, rather than generalizations, are a must due to the different fact patterns. Digital markets often raise complex issues of theory and evidence, challenging classical antitrust concepts and approaches including the tendency to measure consumer harm by focusing on price effects.

At the start of 2019, there are numerous antitrust agencies around the world exploring the scope and boundaries of the laws that they enforce. Most are still at the stage of conjecture. They are asking whether existing rules and procedures remain fit for purpose or need to be supplemented with new rules, concepts, enforcement posture, or even regulation.

ANTITRUST AGENCIES AROUND THE WORLD GRAPPLING WITH DIGITAL



Our view is that the existing antitrust toolbox is sufficiently flexible to address antitrust concerns that may arise in the digital economy. Given the risks of interfering with fast-moving markets, agencies must be disciplined, reserving enforcement activity for situations where there is evidence of actual or likely harm.

But the reality is that agencies are now under some pressure — including, in some cases, political — to ensure that they are not missing any potential anticompetitive problems. In the following, we describe likely areas of focus and what compliance steps will help avoid unwarranted scrutiny.

Mergers

The predictive nature of merger-control enforcement provides an opportunity for antitrust agencies to consider and conjure potential new theories of competitive harm. These theories can influence markets to a significant extent — particularly digital markets, where innovation plays such an important competitive role. The European Commission has previously made the headlines for developing a **controversial innovation theory of harm**. We expect this to continue in 2019, meaning that deals in sectors characterized by high levels of R&D can expect to be closely scrutinized when they have the same R&D "direction of travel" in "innovation spaces" — even if market shares or product overlaps suggest few conventional antitrust concerns. Companies need to plan ahead carefully in order to be able to address detailed information requests (e.g., in relation to early stage R&D) and to be able to fend off competitor complaints.

Acquisitions of start-ups/nascent competitors do not always qualify for merger control review and some antitrust authorities have expressed frustration at this. Germany and Austria have changed their merger control rules in order to catch more acquisitions of low revenue targets in certain circumstances. South Korea has stated its desire to do something similar. Some commentators have argued that, instead of being motivated by a desire to achieve faster and better product launches, acquirers aim to "kill" the competition which would otherwise be brought by the target. In 2019, we will see more antitrust agencies working to expand their reach to review this type of deal. Reviewing agencies will demand more explanations from companies about their deal's rationale, particularly if there is a pattern of acquiring certain entities at a certain time. As is typical in any transaction, the story told by deal-related and internal documents will be key.

Data is now seen as the lifeblood of innovation and new entry. Many antitrust agencies have already started to look closely at the acquisition of important data sets (which may overlap with, or be an input for, the acquirer's existing offering). So far, no deal has encountered major antitrust concerns due to data, solely as an input, but there is a sense that antitrust agencies are on guard. It is therefore important that merging parties are able to identify early on whether their transaction may raise data concerns and how these may be effectively resolved. The "4Vs" seems to have entered the vernacular as a practical way (for company and agency alike) to calibrate the competitive significance of a data set: the Variety of data comprising the dataset; the speed at which the data is collected (Velocity); the size of the data set (Volume); and the economic relevance (Value).

Antitrust agencies are also questioning whether the speed and sophistication of price-matching software could make some markets less competitive and **more prone to collusive outcomes**. They worry that algorithms will be so quick to spot a price decrease and respond that the would-be price cutter may not be incentivized to try to win valuable market share in the first place. That kind of effect is difficult to police under general antitrust rules, but agencies could start to look at mergers more carefully to see if the deals might create market conditions which would be conducive to these concerns (higher concentration/transparency etc.). That would see **more consideration being given to a coordinated effects theory of harm** in merger assessments.

Digital coordination

2018 witnessed considerable speculation about how and when pricing algorithms could create competition law headaches for companies. Some of the concerns remain quite fanciful (robots colluding and hiding the evidence), but some more tangible potential risks are emerging.

The first relates to **resale price maintenance** which is effectively illegal in the EU and many other countries. Software which matches or beats the retail price of rivals is generally positive news for consumers. But the same software can quickly identify maverick dealers triggering downward price competition. This leads to an obvious compliance risk for suppliers who must be careful not to cause resale price maintenance indirectly through complaints or pressure.

“ There should be credible evidence of a violation of the law. ...Just because somebody is big does not mean they have violated the laws nor should we in any way just [target them] just because they've succeeded.”

Makan Delrahim, Assistant Attorney General for the Antitrust Division of the US DOJ

Price-matching software can also be used to **implement and monitor "human" price-fixing cartels**. So employees need to be reminded that conduct which would be illegal offline will be illegal online. Using the same third-party platform to determine prices and react to market changes invites an antitrust problem — e.g., a "hub-and-spoke" cartel where the platform acts as a (potentially unwitting) hub coordinating competitors who should be taking pricing and other strategic decisions independently.

Training is key for less experienced employees (who may be under pressure from customers), but also managers (who need to understand the rules). Effective compliance involves a follow-up with spot checks — by interview and through evaluating emails (subject to data privacy rules). While robot cartels are more of a risk for the (distant) future, companies need to understand their algorithms, including what they demand of developers — including the coding of those developers — and the impact they are having in practice.

Market power

High market shares are a normal feature when sectors display network effects (where a product or service gains additional value as more people use it), and vigorous competition takes place "for" — instead of "in" — the market. But concentrated markets and the speed at which new services develop mean that platforms and other major tech companies will receive close attention from antitrust agencies, especially in the EU.

Keeping markets as open as possible will be a prime objective. Agencies will want to ensure that competitors can enter the market, including in niche segments where they can expand in order to compete against larger incumbents. Antitrust investigations are likely in relation to **exclusivity arrangements, restrictions on data portability, measures that affect multi-homing (even when that is free) and self-preference by vertically integrated players**. Companies will need to be able to demonstrate claimed efficiencies. They will need to show that clicks do not simply translate into a demand for low-quality content; to show why limiting entry into the ecosystem increases quality.

Some antitrust agencies are looking at **digital platforms with a dual role**, where they provide a distribution channel for others while marketing their own products. The question, according to the European Commission, is whether platforms gain access to **competitively sensitive information about competitors' products** which could be used to boost their own retail activities to the detriment of competitors on the platform.

Conclusion

Despite this extra attention, agencies will be keen not to dampen innovation and companies should not be deterred from pro-competitive activities. The challenge for business is to understand the impact of often controversial enforcement, including its boundaries and limiting principles so that legitimate conduct is not side-lined. Dialogue with antitrust agencies is also likely to help. Agencies have warned of the need to shape digitalization to ensure that tech continues to work for people and not the

other way around. To many, that smacks of paternalism and hints at a type of intervention that may not be appropriate for a law enforcer. But whatever your standpoint, 2019 could be the year where tech companies are required to step up their communication and advocacy efforts to avoid being shaped by unnecessary enforcement and even regulation.

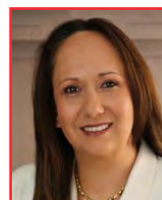
“ This is protecting European consumers. This is our mission, these are our very basic values. In our work on competition, like any good knitter, we have a pattern to follow. ”

Margrethe Vestager, European Commissioner for Competition



Creighton Macy

Partner
Washington
creighton.macy@bakermckenzie.com



Carolina Pardo

Partner
Bogotá
carolina.pardo@bakermckenzie.com



Grant Murray

Director of Knowledge
London
grant.murray@bakermckenzie.com

Taxation of the digital economy

The question of how to make tax rules fit for the digital economy continues to dominate international tax discussions. Large tech firms, particularly online marketplaces, social media platforms and search engine owners, must brace themselves for new tax rules being crafted and implemented in 2019 and beyond. They would be well-advised to monitor developments closely at both international and national levels and review their existing structures as necessary.

The race at international level

The Organisation for Economic Cooperation and Development ("OECD") has for many years been the leading voice in international tax matters and among other things, it spearheaded the most far-reaching modern change to international taxation yet, the Base Erosion and Profit Shifting ("BEPS") project. It has been a key proponent of the view that because the digital economy is increasingly becoming the economy itself, it would not be appropriate to ring-fence it when designing tax legislation. Despite this, a combination of the court of public opinion and a growing need for countries to raise revenues has prompted calls to redesign the international tax system so that it applies effectively to "digitalized" businesses. Achieving such a redesign is far from simple and threatens the underlying premise that has governed the principles of taxation for centuries, namely that companies should be taxed on their profits not their revenues.

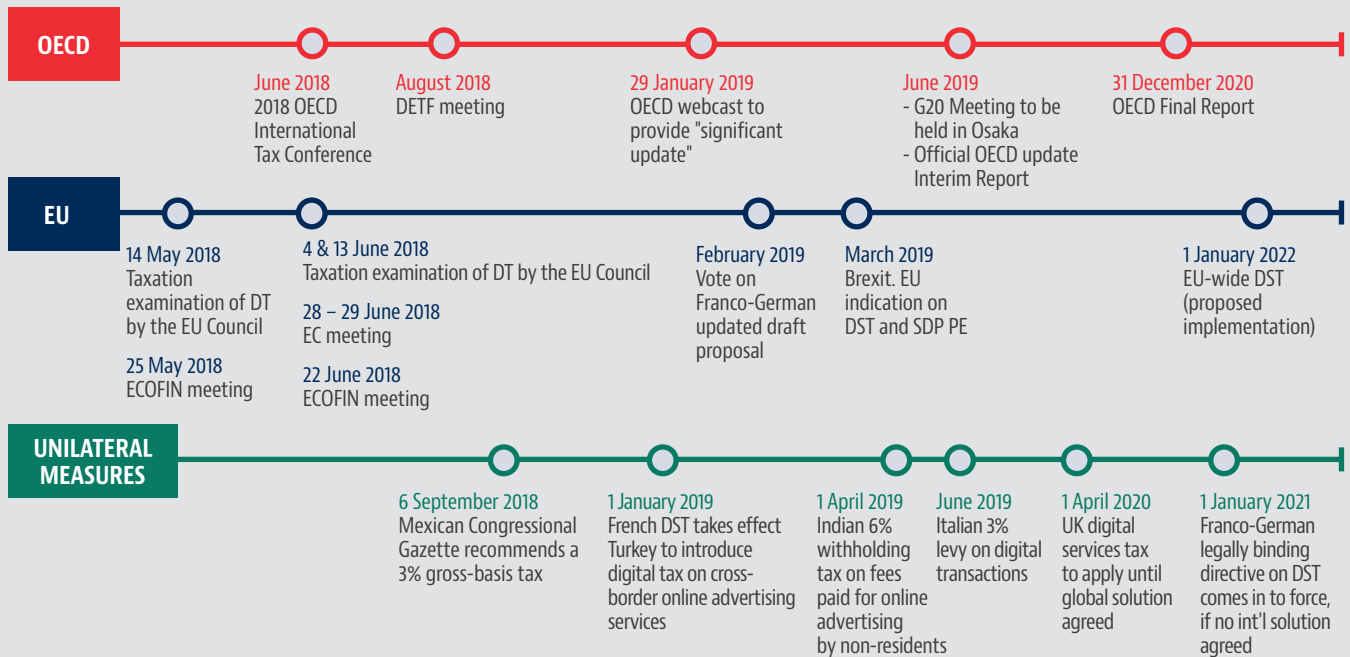
The desire to be the first to achieve consensus on any new basis of taxation has led to an "arms race" between the OECD and the European Commission ("EC") (which is itself an OECD participant). The OECD fired the first shot on 16 March 2018, issuing its [interim report](#) (the "Interim Report"), emphasizing the need for a long-term solution, just days before the EC released both a long-term and an interim [proposal](#) on 21 March 2018. The Interim Report again emphasized that the digital economy could not be "ring-fenced" from the broader economy. In contrast, the EC emphasized the need to target, at least in the short term, certain types of digital businesses, namely, online advertising services targeted at users of digital interfaces; intermediation services enabling users to find and interact with other users (but not communication or payment services); and transmission of data collected about users. This difference in approach between the OECD and the EC initiated a geopolitical battle between short-term and long-term solutions. However, short-term political expediency, in the form of targeting the gross revenues of digital businesses,

risks damaging the OECD's vision of a more long-term and principled answer that complements the existing international tax framework through taxing profits rather than gross revenues.

In theory, the OECD appears to have a lead in this race for now, as the 5 December 2018 meeting of the EU Economic and Financial Affairs Council ("ECOFIN") ended without winning the necessary support from EU Finance Ministers for the EC's mooted Digital Services Tax ("DST"), but the OECD's position is fragile. The ECOFIN meeting did result in agreement to work on a [new joint proposal](#) from France and Germany for a narrower-based DST, to come into force on 1 January 2021. In a more recent development, Romania, which currently holds the Commission Presidency, has proposed instead an EU tax on revenues resulting from the placement of targeted advertising on a digital interface (to include the sale of user data), to come into effect on 1 January 2022. The proposal seems initially to have been well-received and will be further discussed at the March ECOFIN meeting. The EC's proposal to shift from unanimity in tax matters to "qualified majority voting", if accepted, could tighten the race, but the prospect of Member States agreeing to this change currently appears remote.

The OECD in the meantime, in a "Tax Talk" on 29 January and in a short policy paper released on the same day, unveiled details of proposals being considered under each of two "pillars" endorsed by the BEPS Inclusive Framework. The first of these pillars relates to nexus-based approaches involving the allocation of taxing rights, including revising existing profit allocation rules by reference to "active user contribution", "marketing intangibles" or where a "significant economic presence" exists. The second pillar relates to a potential minimum tax, proposing two sets of "interlocking" rules involving an income inclusion rule on profits of related party investors subject to a low effective tax rate and a source country deduction denial rule on under-taxed payments. The OECD followed up with a more detailed Consultation Document, published on 13 February, that sets out these proposals in more detail.

TAXATION OF THE DIGITAL TAXONOMY - TIMELINE



Unilateral country measures

The proliferation of unilateral country measures is also a serious threat to the OECD's role as a standards-setting body that can ensure a fair, certain and consistent international framework. Since the publication of the Interim Report, in September the Mexican Congress has taken steps towards a 3% gross-basis tax and in October 2018, both the UK and Spain announced that they will unilaterally introduce a DST. The Australian Treasury also released a discussion paper in October 2018 on whether taxing rights should change to reflect user-created value, whether the value of marketing intangibles is appropriately recognized by the international tax system and suggesting that profits should be allocated across countries using formulary apportionment. Another recent example comes from France, where the French Minister of Economy and Finance, Bruno Le Maire announced on 17 December 2018 a tax on highly digitalized enterprises, to enter into force on 1 January 2019. This law is expected to closely follow the EC's gross-basis tax proposal, although the draft law is not expected until later in February 2019. Added to this is the Italian Parliament's approval of a tax on digital services that mirrors the EC's DST proposal. The moves by Australia, Mexico, Spain, France, Italy and the UK are particularly noteworthy as all six countries are full members of the OECD.

Outlook

OECD Secretary-General Angel Gurría, in his report to the G20 leaders delivered in Buenos Aires in December 2018 expressed hope that, at the June 2019 G20 summit, the G20 will be able to "celebrate an agreement on the what and how of a long-term solution to be delivered in 2020". It is critical that such a consensus materializes, because if not, we could see even more unilateral measures leading to potential double taxation

and a significant compliance burden for companies as they grapple with different bases of taxation across the world.

This update is a condensed and adapted version of an article by Tom Roth, Kate Alexander and Allen Tan that was first published in the Tax Journal on 8 February 2019.



Kate Alexander

Partner
London
kate.alexander@bakermckenzie.com



Tom Roth

Senior Associate
Singapore
tom.roth@bakermckenzie.com



Jill Hallpike

Knowledge Lawyer
London
jill.hallpike@bakermckenzie.com

Tech companies, ethics and human rights

With the advent of the Fourth Industrial Revolution, the role of the tech sector in modern society has become increasingly evident. Rapid advances in powerful tools such as machine learning, robotics, artificial intelligence and big data promise a world more intertwined with technology than ever, raising questions of ethics, human rights and accountability as technology adopts a far less neutral role in shaping society.

Indeed, questions of social responsibility are being increasingly shifted onto tech companies. From its Silicon Valley mantra of "move fast and break things", the focal point of the industry is being realigned to pay attention to the ethical and human rights implications of technology and technology's impact on society. This is evident in the increasing global reaction against "thoughtless" tech — from the boycott by leading AI researchers of South Korea's top university over AI weapons work, to the pledging of hundreds of Silicon Valley engineers to refuse to build a Muslim database in the United States, it is clear that ethics and human rights are emerging as core tenets of the industry.

The call for an ethical framework

There is ongoing momentum to develop frameworks to guide ethical decision-making by the tech industry.

There have been a number of collaborative initiatives, such as the Partnership on AI, a technology industry body set up to formulate best practices in respect of AI technologies, and the World Economic Forum's Centre for the Fourth Industrial Revolution which focuses on bringing together an "international network of leading companies, governments, civil society, and experts" to design and implement policy and governance frameworks for the technology sector.


The latest development was announced at the World Economic Forum meeting in Davos, Switzerland on 24 January 2019. The Groupe Speciale Mobile launched a guide containing a set of ethical principles to guide behavior in circumstances where there is increasing reliance on digital services by both corporates and consumers. They include commitments to: respect the privacy of digital citizens, ensure protection against cyber threats, the secure

and transparent handling of personal data, addressing online harassment, and ensuring everyone can participate in the digital economy. Over 40 companies have signed up.

Such initiatives evidence a clear trend towards industry commitment to open research and dialog on the ethical and human rights implications of technological advancement on various stakeholders. Organizations that fail to adhere to such guidelines and principles will face increasing scrutiny from regulators, shareholders and consumers.

In addition, other organizations and groups are looking at certification and oversight programs to enable vulnerabilities to be detected.

A lot of this is intended to stem regulatory intervention which will struggle to manage the rapid pace of change and may stifle technological development with limited effectiveness in promoting an ethical and human focused approach to innovation. There is a clear movement for greater regulatory oversight as evidenced by, for example, the European Commission's recently published first draft of its ethics guidelines for the development and use of AI to guide the European Union on its future policy-making in the tech sector.



The enactment of the European General Data Protection Regulation, with its extraterritorial reach, also demonstrates an intention to enhance the protections for personal data and enhance the rights of data subjects in a world in which data is rapidly becoming a very valuable asset. Similarly, growing momentum over data protection and privacy can be seen in China with its first comprehensive privacy standard, the Personal Information Security Specification, which came into effect in 2018 alongside the United State's California Consumer Privacy Act.

Ethics by design

Companies globally have long committed to internal policies framed by data ethics, principles and initiatives, however, we are seeing greater pressure for more to be done to demonstrate greater accountability by the industry to the public.

In particular, ethical design is finding prominence, with the incorporation of ethical principles and values into design. Privacy by design and transparency on how data is handled have been key areas of focus.

Another trend is the move towards an industry "doctrine of explainability" that places responsibility on the industry to ensure those who are impacted by powerful tools such as AI are given the information to understand why and how systems operate in the way they do. Similarly, there is a rising awareness of the effect of biased datasets and the need for greater diversity in the tech workforce to address such biases. Values of fairness and governance are key in the development of ethical design practices.

As regulatory frameworks struggle to keep up, technology companies are being seen as critical to ensuring ethical values and human rights are considered in the development and deployment of new technologies, putting greater pressure on tech companies to take the lead.



Anne-Marie Allgrove

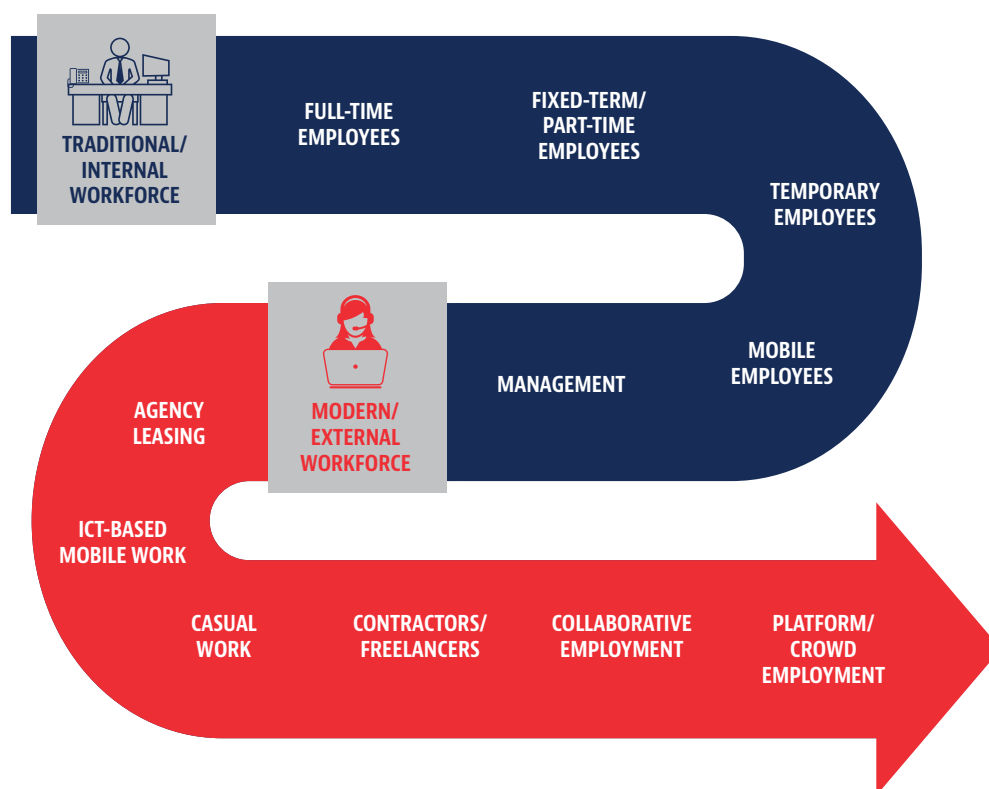
Partner

Sydney

anne-marie.allgrove@bakermckenzie.com

The modern workforce

The nature of work in an increasingly globalized world is perpetually changing due to the rise of contingent workers, increased demand for flexible working schedules, and changing skill requirements and talent pools. Like it or not, this "modern workforce" is here to stay. A 2018 study by Deloitte identified approximately 77 million formally recognized freelancers in Europe, India and the United States alone.



As the modern workforce and the gig economy continue their exponential growth, pressure is building on governments to explore new ways to provide adequate protection and rights for workers and employers. Creating a modern fit-for-purpose workforce is a compliance challenge as regulatory obligations arise across multiple areas, including employment, remuneration and benefits, mobility, data privacy, tax and protection of confidential information/trade secrets. Non-compliance with modern workforce obligations may lead to adverse reputational, regulatory, financial and employee

relations risks. And as early adapters of alternative working models, TMT organizations are often most susceptible to these risks.

Although government responses are still in the early stages, at a judicial level, the level of misclassification litigation intensified in 2018, as gig economy workers challenged their status with varying results. The simultaneous flexibility and autonomy enjoyed by gig economy workers has left them in an ambiguous position, and globally courts have been grappling with how to analyze and label

this evolving workforce, resulting in a number of landmark cases changing the shape of employment law across the globe.

While the issue of "control" over the user was a universal feature of court judgments in 2018, the outcomes of the cases have been anything but consistent.

- **Australia:** Australia recently enacted the Fair Work Amendment (Protecting Vulnerable Workers) Act 2017 to protect against the exploitation of the contingent workforce. The Amendment imposes liability on a franchisor if it knew or could reasonably be expected to have known that its franchisee would breach employment laws, or that a violation "of the same or a similar character" was likely to occur. The framework for determining whether joint liability exists hinges on the degree of influence or control over the franchisee's activities. Liability, however, may not attach if a business takes "reasonable steps" to prevent a franchisee's breach of Australian workplace laws.
- **Italy:** In Italy, in a landmark case, a lack of control was cited as a determining factor for rejecting a claim for employment status by six gig economy food delivery riders.
- **France:** Gig economy workers in France also struggled to successfully challenge their self-employed status in a variety of cases against digital platforms throughout 2018, with the Supreme Court turning this on its head in November 2018 declaring gig economy food delivery riders to be employees, in the first judgment of its kind in the country.
- **Mexico:** The Mexican Federal Labor Law may impose joint liability on two or more companies for labor and social security obligations owed to an employee, including statutory severance. As in the US, in Mexico such risks are further exacerbated when a business exercises strict control and supervision over its contingent workforce. Where a contingent worker files a labor claim against the business, or both the business and the third-party service provider, claims typically allege that the business benefited from the worker's services. In an effort to alleviate this risk, all employment documentation vis-à-vis the contingent workers should refer only to the service provider.
- **Spain:** In Spain, a breakthrough case labelling gig economy workers as employees coincided with collective protests by delivery riders to claim recognition of employee status. This increased Labour Inspection orders to companies to reclassify delivery riders as ordinary employees and an imposition of sanctions and requests for unpaid social security.
- **UK:** The UK continues to grapple with defining the employment status of those working in the gig economy. Employers in the UK face repeated litigation over the status of contingent workers, focused principally on employee misclassification. Misclassification stands at the forefront because workers not classified as employees have minimal employment rights. As a result, contingent workers often do not benefit from statutory

entitlements, including statutory holiday pay and protection against unfair dismissal. The UK misclassification analysis also focuses on the amount of control a company exercises over its contingent workforce. If the company exercises a high degree of control over the activities performed by an individual, that individual may be erroneously classified as a contingent worker and the company may be liable for certain statutory workplace rights. Despite the attention this topic has drawn in the UK, substantial legislative reform and change for such workers have been slow to come.

- **US:** In the US, in what is believed to be the first time a gig economy case has been fully decided on the merits, a California federal judge ruled that a food delivery driver was properly classified as an independent contractor. The court used the multifactor Borello test to analyze whether the driver was an independent contractor, or a misclassified employee. This case was swiftly rendered moot by the California Supreme Court's 30 April 2018 decision in the *Dynamex Operations West Inc. v. The Superior Court of Los Angeles County* case. This decision upended the gig economy by replacing the multifactor Borello test for independent contractor misclassification, with the rigid ABC Test (read more [here](#)).

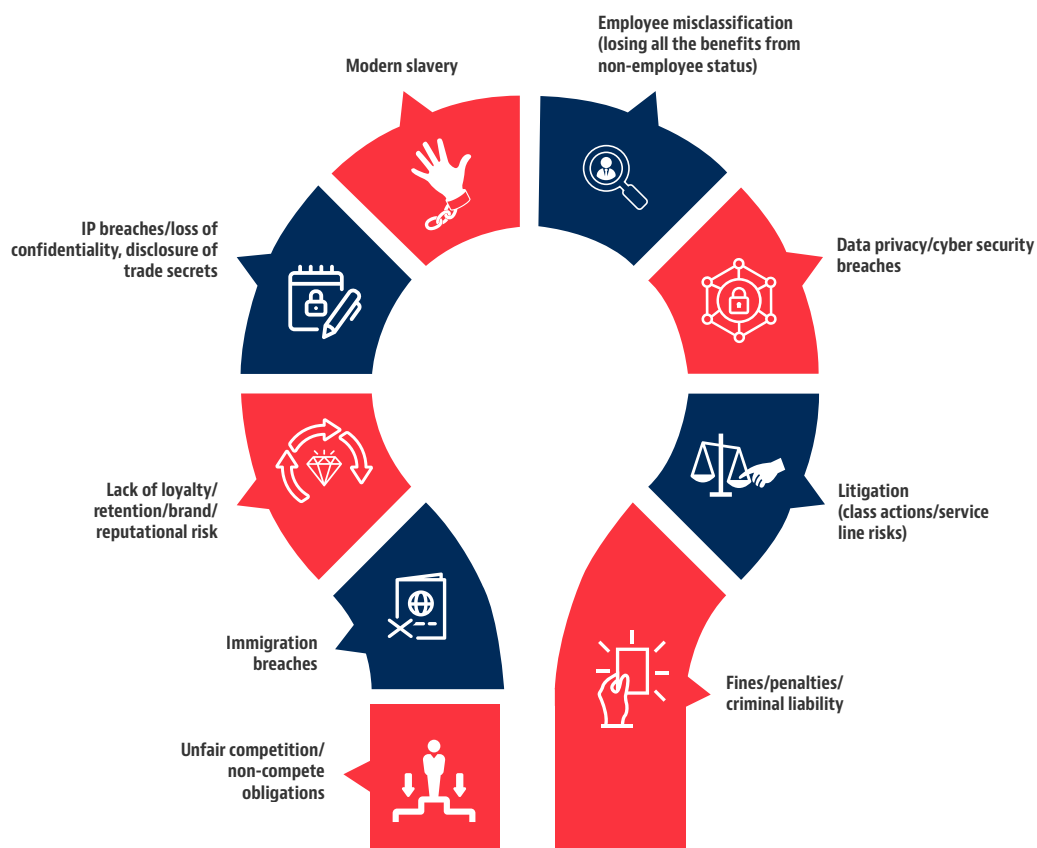
While the prevalence of the gig economy varies considerably across the globe, it is becoming increasingly apparent that traditional employment laws must rapidly evolve to keep pace and provide equitable outcomes for all involved in this rapidly transforming space. Arguably, an intermediate or hybrid status is where gig economy workers would most comfortably sit, and while discussions about regulatory reform have taken place across jurisdictions, no solutions have yet been found and employers can expect uncertainty surrounding gig economy workers to continue into 2019.

Employer to-dos

While integrating the modern workforce into a company's business strategy may be commercially attractive, businesses should be wary of the risks posed by relying on the gig economy to bolster their workforce.

- Mitigate potential claims at the onset through audits and risk management techniques.
- Conduct global compliance audits through expert attorneys who can advise and provide support to address the risks arising across multiple functional areas, such as employment, remuneration, benefits, mobility, data privacy, tax, and protection of confidential information/trade secrets. Obtain practical advice before a joint employer or misclassification claim is alleged.
- Additionally, compliance counseling by a multinational team of attorneys is important to help the company stay abreast of recent developments in this space.

RISKS AND CHALLENGES FACING GLOBAL BUSINESSES AROUND THE MODERN WORKFORCE



Modern Workforce trends and solutions around maintaining or introducing optimal modern workforce arrangements within this constantly changing legal and commercial environment can be found on Baker McKenzie's [**Modern Workforce Hub**](#).



Susan Eandi

Partner
Palo Alto
susan.eandi@bakermckenzie.com



Elizabeth Ebersole

Partner
Chicago
elizabeth.ebersole@bakermckenzie.com



Caroline Burnett

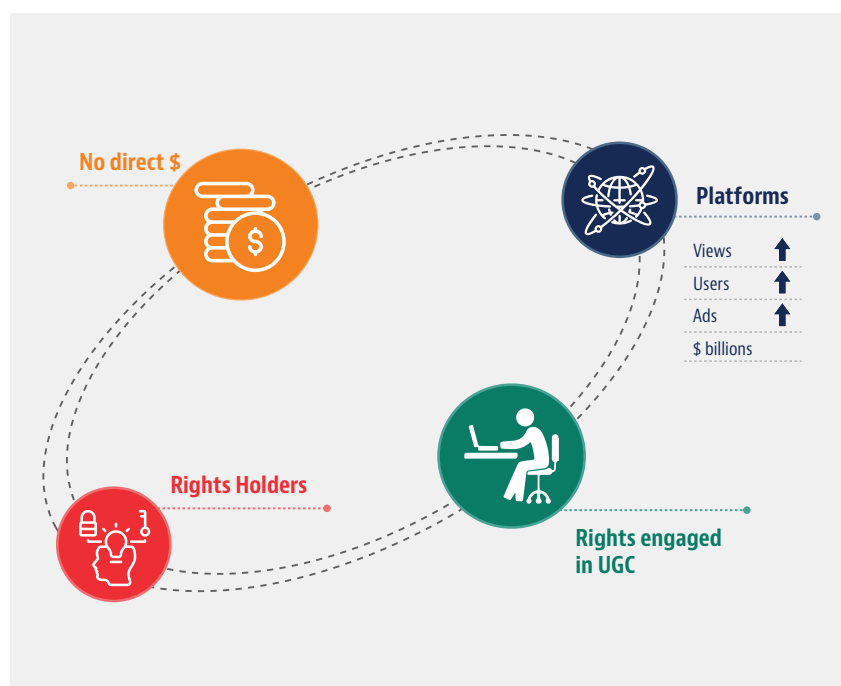
Knowledge Lawyer
San Francisco
caroline.burnett@bakermckenzie.com

Content governance obligations for online intermediary platforms

In the year ahead, the scope and practical operation of the safe harbours relied on by intermediaries is set to be a core battleground in the fight against illegal online content. These "safe harbour" provisions, enacted around the world in the early 2000s, shield intermediaries, including ISPs, social media platforms and other online service providers with user generated content, from claims in relation to the actions of their users, for example claims from rights holders for IP infringement.

Safe harbour provisions

Broadly speaking, safe harbour defences will apply to those intermediaries that do not have actual knowledge of an infringement (or awareness of facts or circumstances which would make such infringement apparent) and, upon receipt of a credible notice, act expeditiously to remove infringing material. Existing laws regulating safe harbours are complex and can differ in critical respects between key jurisdictions. For example, in order to qualify for the hosting defence under EU law, a service provider must only play a neutral, technical role, and not engage with uploaded user generated content (UGC) in any material way. In contrast, US service providers are encouraged to police their platforms in order to avail themselves of the equivalent provision, and measures taken in good faith do not put the safe harbour at risk (the "good Samaritan" clause).



Value gap

Rights holders have long argued that the existing safe harbour provisions no longer reflect the realities of modern technology and platform use. They point to the "value gap" on major UGC platforms. This value gap occurs where users upload infringing content, which if popular can attract millions of views, while adverts run during or adjacent to this content increasing a platform's revenues. In the EU, due to the lack of a good Samaritan clause, proponents of the value gap contend that, intermediaries are disincentivised by the safe harbour defence from taking reasonable steps to combat infringement and also benefit from infringements occurring on their platforms. An accusation is also made that this results in intermediaries indirectly encouraging or at least tolerating such infringements.

"Techlash"

In an age of digitalisation and social media, an increasing number of people rely on the internet for their news and entertainment updates and engage in social media activities. The amount of content created online poses challenges, which range from fake news, terrorist content, hate speech, suicide content to influencer marketing and IP right infringements.

Many consumers are increasingly sceptical towards big tech companies and start to query the benefits of new technologies. The Economist coined the term "techlash" to describe this phenomenon. In a similar vein, governments are starting to question the scope of the existing safe harbour provisions and new legislative concepts, such as Germany's recent Network Enforcement Act, are being developed, arguably shifting, at least in part, the responsibility of pursuing criminal offences in the digital sphere onto social media platforms and subjecting them to significant fines if they fail to perform this task.

EU copyright reform

At the time of writing, the European Commission is in the final stages of confirming agreement of a new Copyright Directive (**Directive**).

The Directive is part of a wider reform by the EU Commission of copyright in the internet age, within its plans to create a digital single market. Its path has been far from smooth so far: the European Parliament, in a first vote of 5 July 2018, rejected an earlier draft of the Directive, after the EU Parliament's (JURI) Committee on Legal Affairs narrowly approved it earlier that year.

The draft Directive was then narrowly approved by the European Parliament in September 2018, and revisions based on the so-called "Voss" proposal, named after German MEP Axel Voss formed the basis for lengthy three-way negotiations among the Council of the EU (which represents the individual EU Member States), the EU Parliament and the European Commission. Following Franco-German talks and further debate in the Council, it was announced on 13 February 2019 that a political agreement had been reached. The Council then confirmed the adoption of an agreed text on 20 February 2019. Notably, the Netherlands, Luxembourg, Poland, Italy and Finland did not support the final package and issued a joint statement in which they called it "a step back for the digital single market" which failed to strike the right balance in protecting rights holders and the interests of EU citizens and companies.

The agreed draft Directive will now proceed to the JURI vote and also requires approval of the EU Parliament which is anticipated to occur in early April 2019. Once confirmed it will be published in the Official Journal of the EU. Thereafter, Member States will have 24 months to transpose the new rules into their national legislation.

The Directive aims to re-calibrate the balance of current protections in favour of rights holders. The draft Directive contains the following highly controversial provisions, Articles 11 and 13, which have been the subject of much debate and campaigning:

1. Article 11: Ancillary copyright of press publishers

The proposed Article 11 will introduce a type of additional copyright for press publishers, separate from the copyright in individual articles. Article 11 has been referred to as "link tax", "news tax", "publishers' right" or "neighbouring right", and follows along the lines of similar laws previously introduced in Spain and Germany. Under the new Article 11 displaying anything other than single words or "very short extracts" of content to users via online platforms and other news aggregators, will require a licence. The underlying rationale of Article 11 is to generate income for (European) press publishers in an attempt to address a perceived "value gap". Campaigners against its introduction argue that it will limit freedom of expression and access to information.

2. Article 13: Content upload filters and requirements to license or prevent illegal materials

Equally controversial is the draft Article 13, which states that certain service providers are engaged in an act of communication to the public in respect of UGC containing copyright material. This results in an effective obligation for those platforms to monitor UGC, which is contrary to the safe harbour provision set out in Article 15 of the E-Commerce Directive.

Article 13, in its currently agreed form, places platforms under a responsibility to enter into licences with rights holders in respect of content shared on the platform. If unlicensed content is shared, platforms must be able to demonstrate they have made "best efforts" to obtain licenses from rights holders.

The workability and scope of such a compulsory license scheme has been the subject of debate and raises many questions. Would platforms need to have blanket licences in place with every rights holder in the world? If such licences were meant to cover specific instances only, would the licence only cover that piece of content? Alternatively, would the parties be required to revisit the licence each time additional content is identified?

Article 13 requires that "best efforts" are made "in accordance with high industry standards of professional diligence to ensure the unavailability of specific works and other subject matter for which rightholders have provided the service providers with the relevant and necessary information". Critics fear that Article 13 will require the use of upload filters, which could lead to the over-blocking of legitimate content. As the media has widely reported, this could also affect the sharing of satirical content

and memes where these are based on copyright protected images, potentially impacting freedom of expression. Mr Voss has been cited as arguing that Article 13 does not require upload filters as a means of compliance. However, it is hard to avoid the conclusion that the Directive in practice will materially change the current safe harbour laws in Europe, despite the Commission's position that this was not the intention of the originally proposed Article.

Also contentious is that Article 13 includes a carve-out for SMEs from the obligation to ensure unavailability of copyright works, which would in essence amount to a new safe harbour for smaller platforms. Qualifying smaller companies would only have to make best efforts to obtain a licence and take down illegal content. This is purportedly to help lower the barriers to entry for new platforms and applies only to those SMEs that are younger than 3 years old, with an annual turnover under €10 million, and with fewer than 5 million unique visitors per month.

Changes to safe harbour regimes in Australia and Thailand

Australia recently extended its safe harbour regime, which currently protects only a narrow class of carriage service providers such as telcos and ISPs, to organizations operating in the disability, educational and cultural sectors. More on the background to the changes is available in our client alert [here](#).

The amendments limit the scope of remedies available against service providers operating in these industries who implement notice and takedown procedures to remove infringing material and who otherwise comply with the conditions in section 116AH of the Copyright Act 1968 (Cth). The amendments do not operate to extend the safe harbour regime more broadly to any service provider who offers, hosts or aggregates content online. They represent the Government's first step to incremental safe harbour reform and it will be interesting to see if further copyright reforms are forthcoming in 2019.

Thailand is also looking to reform its Copyright Act 1994 in order to speed-up the removal of illegal online content. Proposed changes would require internet service providers to block users who repeatedly share infringing content online and implement standard technical measures to detect infringing content. The proposed new copyright laws are based on the US Millennium Act and would allow rights holders to ask platforms to remove infringing content without the need to seek a court order (as currently required) while at the same time, providing platforms with a safe harbour against infringement lawsuits.

Future trends

For intermediaries it is clear that the safe harbour provisions will continue to come under pressure, not least due to the technological developments in the field of artificial intelligence and machine learning, which (arguably) increase intermediaries' ability to "know" what is on their platforms. At the same time, machine learning is not free from drawbacks, as it is potentially inefficient and vulnerable to spoofing. Last but not least upload filters and any other monitoring of UGC will lead to arguments as to their affect on basic human rights, such as freedom of expression.

In the EU markets, at least, platforms will be working to get ahead of the implementation of the Copyright Directive and looking carefully at any changes that will need to be made to their business models in order to protect their revenues.

For a more detailed commentary on EU and US laws on intermediary liability and many of the issues identified above two of the authors of this article (Ben Allgrove and John Groom) have contributed Chapter 25 to Tanya Aplin's upcoming new book *Handbook for IP and Digital Technologies* (working title; to be published in late 2019).



Ben Allgrove

Partner
London
ben.allgrove@bakermckenzie.com



John Groom

Senior Associate
London
john.groom@bakermckenzie.com



Birgit Clark

Knowledge Lawyer
London
birgit.clark@bakermckenzie.com

Data is king but compliance is key

There is no question that data is a critical asset for any business seeking to compete and thrive in today's globally connected economy. **Monetising data** is a must. However, **personal data regulation** will continue to develop in numerous countries around the world, with more (albeit slow) alignment between different regulatory regimes expected. At the same time, regulators will step up enforcement activities. Moreover, 2018 has shown that the role of data in economic markets and the societal impact of widespread data gathering and usage goes well beyond traditional data privacy concerns. 2019 will be the year in which data will continue to move from an issue of primary interest to privacy regulators (and privacy practitioners) to an issue of common focus for regulators and practitioners from other disciplines such as antitrust and tax just to name a few. This, coupled with further shifts in consumer behavior and expectations towards data monetisation, will significantly increase the risk profile of non-compliant data handling.

On a related note, **data centers** will continue to play a key role for many businesses. We expect an increase in edge data centers as well as all-flash technology. Tech companies will continue to work towards their commitment to power their data centers completely with renewable energy, and security will be an important issue in 2019 and beyond.

Data monetisation - shifting tides

That data is a critical asset for any business seeking to compete and thrive in today's globally connected economy has long been without question. However, for many years, thinking surrounding data by both businesses and, to some extent, regulators largely appeared to follow a fairly simple path. Businesses sought to both grow and control data sets of increasing value. Regulation focused primarily on privacy concerns for individuals.

While cracks have been appearing in this approach for some time, 2018 felt like the year where things fundamentally changed. Some of this change was clearly driven by high profile data breaches and other data-related concerns receiving widespread attention. However, change has also inevitably accelerated as the complexity of issues surrounding the collection, use and control of data has become more evident, with data being a key asset and driver in the digital world.

So, what are the key issues and trends likely to be impacting data monetization in 2019 and are we likely to see further shifts in consumer behavior, regulator activity and other government intervention?

Changing consumer expectations

With the public fallout of major data breaches continuing to make global headlines throughout 2018, it is unsurprising that consumer concerns around how individual consumer data is used and shared have grown.

The resulting loss of consumer trust has been felt widely in some sectors, and is likely to continue to drive both consumer behavior and business and regulator responses in 2019. This is also true from a litigation perspective, since consumers are becoming more aware of their rights and willing to enforce them via available avenues. Companies should therefore get prepared to address claims and actions, from consumers as well as regulatory authorities. Needless to say that the negative impact in terms of reputation may have critical consequences.

Global regulatory responses have varied, but as we move into 2019 and the first fines under the GDPR are issued, the ripple effect of stricter privacy regulation in Europe is likely to continue to be felt elsewhere as other jurisdictions consider the implementation of more stringent privacy measures, such as a "right to be forgotten" or "right

to be deleted". Meanwhile, some jurisdictions are experimenting with other means of tightening control over data, including data residency requirements.

Data portability

Whilst stricter privacy regulation restricting unfettered data usage and disclosure continues to evolve, greater access to data is also a trend, and opening-up of previously tightly held and controlled data sets is a key driver for governments in many jurisdictions with a number of consumer-driven data portability regimes being proposed or coming into effect.

Greater rights for both individual and business customers to access and direct transfers of data held by service providers are being pursued in a number of countries by governments chasing innovation, competition and consumer benefits from the opening of previously siloed datasets held by incumbent operators.

While, on the one hand, these rights foster innovation and new business opportunities, on the other hand, they can sometimes raise concerns around use for unintended purposes.

Open data and data-driven innovation

On a similar theme, other means of driving positive innovation and collaboration through increased sharing of data are being explored in many places. From the opening-up of government-controlled datasets to incentives for increased collaboration and sharing between academic institutions and the business community, governments are seeking ways to unshackle innovative developments that have previously been hamstrung by a lack of access to usable data.

Beyond privacy

If 2018 was the year of GDPR implementation, 2019 is increasingly framing as the year of the competition regulator. Whilst stricter privacy regulation and enforcement will remain a key focus, other - arguably more aggressive - regulators are increasingly seeking to assert themselves in this space.

Significant competition law enforcement actions in connection with business use of data have been undertaken in recent years and competition and consumer regulators and commentators in Europe, and in other jurisdictions such as Australia, continue to debate data-related issues including issues arising from:

- market power and dominance associated with control of extremely large datasets including relevant considerations in the context of M&A activity
- consumer law concerns (as opposed to privacy-specific concerns) arising from:
 - data handling
 - representations made to consumers with respect to data handling
 - the manner in which privacy terms are imposed on consumers
 - consumers' ability to make informed decisions regarding handling of their data
 - information asymmetries between consumers and businesses with respect to business data handling
 - use of data as a "currency" to access services/products/benefits.

As these discussions continue to gather force, data will continue to move from an issue of primary interest to privacy regulators (and privacy practitioners) to an issue of common focus for other regulators and practitioners. Just to mention some:

- digital taxation rules are stretching jurisdictional boundaries to capture online data monetization initiatives
- issues surrounding the IP ownership/control of large data sets is on the radar of major players in the data driven arena.

Ethics bringing a new dimension

As if that is not enough for businesses to grapple with, governments, policy makers, market players and individuals are increasingly bringing ethical considerations into the picture. Beyond compliance, stakeholders are being called to consider ethical implications of their actions. The imminent focus is on AI technology but ethical handling of data will soon be expected more generally. This is not a matter of legal compliance (we are still at an early stage, even if things are moving, especially in Europe), but arguably equally critical since it affects consumer trust.

Outlook

So, if anything is certain in 2019, it is that the role of data in economic markets and the societal impact of widespread data gathering and usage will continue to generate multi-disciplinary questions, complexities and challenges for governments, businesses, academia and other commentators and, more broadly, for society at large. We will continue to see tighter restrictions on data handling whilst, in parallel, the trend of opening access to previously tightly-held data sets will continue.



Allison Manvell

Counsel
Brisbane
allison.manvell@bakermckenzie.com



Adrian Lawrence

Partner
Sydney
adrian.lawrence@bakermckenzie.com



Francesca Gaudino

Partner
Milan
francesca.gaudino@bakermckenzie.com

Personal data regulation — trend spotting

What is expected for the next wave of personal data regulation and how can organizations get ready? Here are our predictions.

The number of jurisdictions enacting a comprehensive personal data protection regime will grow. Organizations subject to these new regimes will need to implement compliance programs to discharge their obligations under the new laws. While recent GDPR implementation experience will be useful, and some personal data compliance policies and practices are suitable to be rolled out across jurisdictions, organizations need to be mindful that requirements between jurisdictions differ and implementation programs will need to be adjusted accordingly. There is no one-size-fits-all approach.

Here are three examples of new comprehensive personal data regulatory regimes.

- In **Brazil**, organizations should be getting ready for the commencement of the GDPR-inspired Brazilian General Data Protection Law in August 2020. A sensible first step for businesses operating in Brazil would be a data-mapping exercise in order to understand current data processing activities, identify gaps and vulnerabilities and then establish a compliance plan.
- In the second part of 2018, **India** released a draft Personal Data Protection Act containing a comprehensive personal data protection law (detailed analysis [here](#)). Features of the draft law that quickly drew attention included the three categories of personal data and how on-soil requirements apply to those categories. The draft is under review.
- **Thailand** for several years has been developing a Personal Data Protection Act. In September 2018, the government issued a new draft with some GDPR-like features and it is now expected that the government will move with speed to enact the new law.

Established personal data regimes will continue to be reformed. Organizations operating in jurisdictions that already have comprehensive personal data protection regimes need to keep on top of the next wave of reforms. For example, in the **United States**, the California Consumer Privacy Act ("CCPA") is already bringing profound changes ahead of its 1 January 2020 effective date, given its 12-month look-back provision to January 2019 ([click here](#) for our analysis of the impact of the CCPA on consumer goods and retail businesses; and [here](#) for an analysis of its impact on employers). Also, consumer data protection statutes in Colorado and Vermont, for example, have recently entered into effect. Governments of other states, such as Washington, Massachusetts and New Jersey, are considering or introducing similar legislative proposals.

“ The US experience illustrates the immense challenge lawmakers may face in trying to get the balance right between protecting individuals and supporting business development. ”

Lothar Determann | Partner, Baker McKenzie

“ It is imperative in forward-planning for personal data compliance to appreciate that the evolution of personal data protection laws did not stop with the GDPR. ”

Anne Petterd | Partner, Baker McKenzie

Another example is **Singapore** where a review of the Personal Data Protection Act 2012 is underway. Contemplated changes include requirements on breach notification, spam and do not call marketing requirements. Organizations will need to monitor developments in order to ensure compliance with new requirements, but also to be able to contribute to public consultations (e.g., to ensure the business impact of a proposed changes is understood by regulatory authorities).

Data residency requirements will be a key business expansion issue. Several new and under-development data protection laws have a requirement to keep certain personal data within the jurisdiction. This is the case, for example, for China, Vietnam, India and Indonesia. On-soil requirements are a particular challenge for businesses that largely operate online and do not typically set up technology infrastructure in each jurisdiction where they offer their products or services. "Is there a relevant on-soil or data localization restriction?" needs to be a question included in business expansion plans to a new jurisdiction.

Differing personal data regulatory requirements among jurisdictions will be an area of focus for lawmakers and we expect more alignment. Take the US as an example. Concerned about the sprawl of state consumer data privacy legislation,

federal legislators, companies and industry associations have expressed support for a superseding federal privacy law. Several federal bills have been formally introduced, including the Data Breach Prevention and Compensation Act introduced in January 2018, the Data Care Act introduced in December 2018 and the American Data Dissemination Act introduced in January 2019. Other federal proposals have been circulated informally. For its part, the Trump administration had the National Telecommunications and Information Administration ("NTIA") publish the outcomes and goals that should be the focus of any federal legislation. The Federal Trade Commission is one of the over 200 parties to submit a comment on the NTIA's proposed framework. The FTC's comment received sharp criticism from privacy watchdog groups, in particular the FTC's statement that a default consumer opt-out of online advertisements would not be appropriate as it would likely result in "the loss of advertising-funded online content".

Additionally, businesses and industry groups, such as the US Chamber of Commerce and the Business Roundtable, have released federal legislative proposals all of which would preempt the CCPA and other similar state laws. The US experience illustrates the immense challenge lawmakers may face in trying to get the balance right between protecting individuals and supporting business development.

Growing validation of legal systems as having adequate personal data protection measures. Many personal data laws (e.g., the GDPR) permit cross-border data transfer if the destination country has adequate personal data protection laws. Reliance on these provisions to date has been constrained by the limited recognition between jurisdictions of the adequacy of laws, which in turn is a potential trade obstacle. An expected focus area of governments is convincing their counterparts in other jurisdictions to recognize the adequacy of the destination country's personal data protection laws.

Organizations will want their badges too. An organization-specific certification regime is increasingly being used in conjunction with a government-to-government arrangement to recognize the destination jurisdiction's laws as adequate (e.g., the US-EU and US-Swiss Privacy Shield). As at January 2019, eight jurisdictions are participating in the APEC Cross-Border Privacy Rules (CBPR) (being the US, Mexico, Japan, Canada, Singapore, the Republic of Korea, Australia, and Chinese Taipei). CBPRs provide a single framework for the exchange of personal information among participating economies. An organization certified by an Accountability Agent as CBPR-compliant in one jurisdiction can have that certification recognized in other participating jurisdictions. There are also a growing amount of jurisdiction-specific certifications that can be sought for personal data regulatory compliance (e.g., the recently launched Singapore Trustmark certification).

With all these certifications available, a dilemma for organizations is which certification(s) to seek. Among other factors, this will likely depend on organizational footprint, resources needed to seek the certification, recognition of the certification and perceived value to the organization of obtaining the certification.

Regulators will get tougher on businesses with poor data protection practices. Penalties are getting higher for data breaches when an organization is shown to have poor data protection and management practices. Key deficiencies being called out by regulators include poor security protection and incident response practices and lack of responsibility taken by data controllers. Regulators in some industries (e.g., the financial services and insurance industries in Singapore and Malaysia) have recently issued or intend to issue specific instructions on security protections that regulated organizations are expected to implement. Organizations failing to take note of these instructions will do so at their peril if being investigated for a data breach. We predict adequate protections will be regulators' area of focus around the world. In Europe, GDPR enforcement is ramping up with the first hefty fines emerging and more expected. We expect regulators in Europe to focus, among other things, on consent practices and transparency requirements and influential tech companies will be a prime target.

Automated individual decision-making and profiling will be a focus area for regulatory development. Lawmakers and privacy regulators in several jurisdictions are working on setting frameworks for allowing use of personal data in automated individual decision-making and profiling. In some instances, this is part of GDPR implementation activities. But setting a framework for conducting automated decision-making and profiling (or a broader use of personal data in AI) has also been taken up by lawmakers outside the EU. Development of laws in this space may take some time and

this creates regulatory uncertainty for organizations. That said, one emerging theme is that a governance framework for use of personal data in AI is needed urgently.

Data security breach notification requirements will emerge with increasing significance. Jurisdictions will continue to adopt more expansive data breach notification requirements with lower risk thresholds and faster timelines for notifications to authorities and individuals. This will continue to put pressure on organizations' data protection programs as a breach notification to an authority will be a lead-in to a possible enforcement action. Complexities abound in these situations, particularly because companies scrambling to investigate a potential incident may unknowingly stumble across data protection, blocking statutes, and other local restrictions that come into play. Organizations are therefore well advised to work through multijurisdictional "table top" exercises so as to have a better chance of managing such possible incidents well.



Anne Petterd
Partner
Singapore
anne.petterd@bakermckenzie.com



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



Brian Hengesbaugh
Partner
Chicago
brian.hengesbaugh@bakermckenzie.com

Global data center trends

Demand for, and usage of, various types of real estate assets tends to be somewhat slow to change, varying based on macro-economic conditions and other societal changes. However, data center demand and usage change much quicker due to their close ties to technology, media and telecommunications. Here are our anticipated developments and trends around data centers for 2019 and beyond.

Renewable energy procurement

Data centers consume an enormous amount of energy: they are responsible for as much as 2-3% of worldwide energy consumption, primarily driven by cooling and operational needs. Some of the largest data centers use as much power as major cities. A leading search provider has estimated that a single internet search request uses enough energy to light a 60-watt lightbulb for 17 seconds. As global data traffic exponentially increases, so will demand for energy.

Over the past few years, data centers have become increasingly powered by renewable energy resources such as solar and wind power. Renewable energy provides a solution for two primary demands of data centers: (i) it supports the ambitious clean energy goals established by owners and users of data centers; and (ii) it provides a steady energy source at a long-term fixed rate, avoiding the volatility of the traditional retail energy market.

Many of the largest data center owners and users are tech companies. These increasingly have internal mandates to power their data centers completely with renewable energy, and many of them achieved that goal in 2018. In February 2018, one cloud giant announced that it would be partnering with a leading asset management firm to construct a solar array in Nevada that will be the largest anywhere outside China, generating enough power for the equivalent of one million homes.

Data centers procure renewable energy through a variety of methods, from on-site, third-party-owned solar arrays that feed power directly to the data center, to more complicated partnerships with the local utility provider where the terms of the energy procurement are housed in a "virtual" or "synthetic" power purchase agreement and the related solar or wind generation facilities are geographically remote from the data center.

2019 promises to be another banner year for development of renewable energy resources for data centers. Despite reaching its 100% renewable energy target in 2018, one leading search provider recently announced an initiative to be "carbon-free" on a 24/7 basis, meaning that it will attempt to completely eliminate use of fossil-fuel power sources such as natural gas. This can be challenging during periods when renewable resources are inadequate or nonexistent (e.g., night-time or cloudy days for solar energy resources). We expect that as peer companies achieve their initial renewable energy targets, becoming carbon-free will become the next major goal.

The regulatory frameworks and restrictions on energy markets, and renewable energy in particular, will continue to present challenges to the growth of new renewable energy resources for data centers. While major players will continue to create new markets and drive utilities to adopt rules that are friendly to renewable energy, smaller data center developers with renewable energy targets may not have the same opportunities to do so and will be confined to areas with established clean energy markets. As consumers and data center users increasingly demand that their services be supported with clean energy, however, alliances and industry groups such as the Renewable Energy Buyers' Alliance are harnessing the collective demands of these major energy consumers to advocate for market and regulatory changes that will hasten the rise of data centers powered completely by clean energy.

Edge data centers

Over recent years, many industry leaders have spoken about the importance of edge data centers. Generally speaking, edge data centers are typically seen as smaller facilities which are closer to end users than they might otherwise be. The primary benefit of being closer to end users is that services can be delivered quicker, with less latency. The internet of things (connecting various every day objects

to the internet, such as cars and devices) has been one driver of the need for this decrease in latency. As the internet of things has grown, so has the need for processing information with less latency, as decisions may need to be made faster than would be possible if the relevant data center were extremely far away. During 2019 and beyond, we expect an increase in edge data centers.

Security

Security is, of course, not a new issue. However, given the significant repercussions for security breaches, we continue to expect security to be an important issue in 2019 and beyond, and worth discussing. In the data center context, this is primarily relevant in a physical security context. Regardless of the type of data center, ultimately there is someone responsible for physical security. When negotiating to buy a data center, lease a data center, utilize colocation space, lend to a data center owner, etc., the buyer/operator/user/lender needs to understand what physical security and security procedures are in place, whether records are available to confirm such security procedures were followed, and whether there are any potential vulnerabilities.

Storage technology

As technology advances and the acquisition cost is beginning to decrease, all-flash technology is beginning to replace a portion of spinning disk storage. As all-flash storage usage increased, data center development and size could be significantly impacted. In particular, power usage, cooling usage and required space for a particular amount of storage space is often less when utilizing all-flash technology. As a result, if all-flash storage does eventually replace a large portion of spinning disk storage, power systems and cooling systems may be adapted accordingly, and typical data center size (in terms of building square footage) may be decreased.



Jeff Russell
Counsel
San Francisco
jeff.russell@bakermckenzie.com



Brian Zurawski
Partner
Chicago
brian.zurawski@bakermckenzie.com

Looking at China

Chinese tech companies' global influence will continue to grow as they further expand beyond the domestic market and increase foreign investment. China is working to outpace the US and the EU in innovation in many fields including intelligent manufacturing, the "Internet of Things", 5G mobile technology, robotics and AI. Nonetheless, there will be some obstacles in the way, such as a tightening of foreign investment rules, the impact of US/Chinese tariffs, and increasing political pressure on Chinese 5G network equipment.

The growing influence of Chinese tech companies

China and tech

China is home to nine of the world's 20 largest tech companies by market cap, including three in the top 10. Less than six years ago it had two. By contrast, the US has 11 (versus nine in 2013). These Chinese tech giants, along with a few ambitious start-ups — are now shaping business models in Silicon Valley.

Most of these companies have grown into massive conglomerates due to the huge size of the Chinese domestic market and their investment in technology and new business models. Many are now seeking to expand significantly beyond China and are directly competing with well-known counterparts in the West. A number of Chinese tech companies have launched IPOs at home and overseas in recent years and have become major global players.

The domestic environment for Chinese tech companies

The Chinese tech ecosystem is characterized by strong energy and intense competition and this is driving innovation in China.

China has some key advantages to the West in tech, and especially AI, namely the availability of rich data pools to train AI. With less regulation of data collection and use, as well as government-driven data collection policies, China has access to huge datasets on its citizens that don't exist in other countries.

China's technology giants and younger tech start-ups have benefited from blocking and other nationwide measures that have restricted foreign competitors in a market hungry for internet

products. For example, a number of major non-Chinese search engines and social media platforms are currently blocked in China. The great firewall also hands Beijing far greater control over the internet than its Western counterparts.

Beijing is also working closely with some of the largest established technology companies to have joint labs for research and development with government entities. Also, China's largest technology companies as well as leading Chinese telecoms groups are working with local governments on smart city initiatives to optimize traffic flow and prevent and detect crime courtesy of surveillance cameras.

Chinese investment strategy — Made in China strategy and AI plan

China has been working for some time to transform its economy from a capital and labor-intensive manufacturing-led economy fueled by foreign investment to one that is innovation-led and consumer-driven.

These changes were foreshadowed by two high profile strategic plans announced by the Chinese Government: 2015's **Made in China 2025 strategy** and 2017's **Next Generation AI Development Plan (AI Plan)**. The first focuses on foreign investment in technology companies to upgrade Chinese core industries, while the second is an ambitious plan to invest in AI to bring China up to speed with the West within three years and lead the world by 2030.

Accordingly, China is working to outpace the US and the EU in innovation in many fields including intelligent manufacturing, the Internet of Things ("IoT"), 5G mobile technology, seed breeding, robotics and AI. Investments in infrastructure such as AI, IoT and 5G are estimated to reach hundreds of billions of yuan in 2019.

Also, a CB Insights report from 2018 highlights that China has now overtaken the US in terms of global VC start-up funding for AI projects (48% v 38%).

Chinese tech companies as investors

More big Chinese tech companies are going public these days than American ones, with significant investments made by the

Chinese tech majors, many of whom are pursuing IPOs of their portfolio companies. Silicon Valley majors by contrast often acquire companies outright and integrate them into their existing business.

Together, some of the largest Chinese technology conglomerates have funded 45% of the 77 Chinese companies that researcher CB Insights values at USD 1 billion or more.

Ties between the private sector and the Chinese government are further cemented by financing flows with state-owned entities often among anchor investors in technology IPOs.

Overseas expansion

After years of rapid growth in China, some Chinese tech firms are now looking to continue expanding in overseas markets and require more capital to do so.

As they mature, China's tech giants are also opening research facilities overseas and focusing on areas like AI and self-driving cars. Certain of China's search engines aim to increase the number of users that come from outside China and have, to this end, established research facilities in the Silicon Valley and the West Coast.

Chinese foreign investment — 2019 challenges

Beyond traditional competitive issues, Western economies' concerns with Chinese foreign investment include alleged forced tech transfer and protectionism. The close and interdependent relationship between the Chinese state and privately owned Chinese tech conglomerates has also been another area of attention. This close state/enterprise relationship is increasingly complex and nuanced as these companies have become an integral part of modern Chinese life.

This section summarizes some of the headwinds to watch in 2019.

- **Further tightening or changes in Foreign Investment screening rules** — the changes already made have hit hard, with at least 21 Chinese acquisitions cancelled by foreign regulators in 2018. A number of US deals have been delayed or vetoed by CFIUS (Committee on Foreign Investment in the US) — an inter-agency body that screens foreign acquisitions of US

assets for potential national security risks. In August 2018, CFIUS was given expanded jurisdiction to review new categories of foreign investments and US export controls were renewed and tailored to address forced technology transfer concerns.

This was also the result of continued restrictions on outbound transactions in China, and a tense bilateral relationship between China and the US.

- **Impact of the US/China trade war tariffs** — following a report from the Office of the United States Trade Representative into China's reported trade practices under S301 of the Trade Act of 1974, the Trump and Xi administrations are engaged in a tit-for-tat trade war applying customs tariffs on each other's imports. In addition, there are new proposed export restrictions (issued November 2018) on additional technology sectors considered crucial to national security. AI, machine learning, data analytics, aerospace and robotics are among the identified 14 categories of new technologies. The cumulative impact of these measures is starting to flow through to consumers (in terms of price rises) and the wider global economy in 2019.

Investors are closely watching whether China and the United States can reach a trade deal in current negotiations that would lift some of the global gloom. US tariffs have increasingly weighed on Chinese exports in recent months, impacting on business and consumer confidence.

- **Changes to EU Competition Law and Foreign Investment rules** — the Wall Street Journal reports that concerns about the might of Chinese companies and their support from the State is prompting the European Union to reassess its competition rules with an eye to allowing large mergers in order to better respond to foreign competitors. Germany, other EU countries and the EU itself have established processes for reviewing foreign investments modelled on CFIUS.
- **Increased scrutiny of Chinese 5G network equipment** — despite the success in 5G deployment domestically, Chinese telecom equipment giants have faced regulatory push-back abroad and are facing increasing scrutiny of their security practices among foreign governments, some of which are reviewing whether their 5G networking equipment poses national security issues.

Conclusion — growing influence despite the challenges?

As recently highlighted in our client alert [here](#), the pipeline of pending transactions suggests continued divergence in 2019. Chinese investment looks to be robust in Europe in the first half of 2019, with more than USD 20 billion of pending transactions at the

beginning of the year. The pipeline in North America remains weak with less than USD 5 billion of pending deals.

Owing to the challenges China's tech companies are facing in overseas markets due to trade tensions and dampening consumer spending at home, commentators might expect the rapid growth in market cap and revenue of Chinese companies to slow down. However, despite the fact that China's government just announced that its economy grew 6.6% in 2018 (its slowest pace in 28 years and lower than a revised 6.8% growth in 2017), this was in line with analysts' expectations and some of China's largest stocks continue to perform at market-leading levels.

Given the large dimension of many of the big Chinese tech companies, their growing R&D spend, vast domestic consumer base and appetite for investing overseas, Chinese tech companies' influence is likely to continue to grow.



Howard Wu
Partner
Shanghai
howard.wu@bakermckenzie.com



Paolo Sbuttoni
Partner
Hong Kong
paolo.sbuttoni@bakermckenzie.com



Dominic Edmondson
Senior Associate
Hong Kong
dominic.edmondson@bakermckenzie.com

Trade wars to unfold and supply chains to change

The ongoing trade wars between the US and China will continue to impact tech companies forcing them to rethink their supply chains and investment decisions. In addition, TMT businesses will continue to move away from a linear supply chain model towards a **circular economy model or closed-loop supply chain model**. This is in response to a growing world population, scarcity of resources, shorter product lifecycles of electronic devices, a steadily growing volume of electronic waste and changing consumer behaviors.

Trade wars and their impact on supply chains and sales

Trump trade wars and the impact on supply chain and sales

Tech companies are starting to feel the impact of the US–China trade war. Many tech companies produce their consumer electronic products in China or at least source the various product components, such as semiconductors, from China. US tariffs affect precisely these products, including smartphones, smart home devices and wearables imported from China.

Executives and decision-makers from the private sector claim that the ongoing trade wars will impact supply chain and investment decisions. Many US firms responding to the uncertainty will reorganize their supply chains and locate low-cost production in "safe" countries like Vietnam, Malaysia, Indonesia, Mexico and Peru. There's no guarantee they will move much production back to the United States. Likewise, Chinese firms that buy high-tech industrial inputs from the United States will move some of the production to "safe" countries like South Korea, Canada and Australia. But Chinese firms could be inclined to produce many of these inputs at home, even though the cost will be much higher.

5G is widely reported to be a key reason for the trade war. Currently, the race to develop 5G is heating up with major technology companies and telecom operators from Europe, China and the US all involved in the sprint. Mobile internet requires technical "standards" that can be agreed upon globally so that companies that make telecoms equipment, as well as mobile carriers, can efficiently roll out the technology worldwide. The specifications for 5G were agreed upon in December 2017 and June 2018. China is also able to take the lead in 5G development as it only has few large 5G telecom operators in the country with government support. In the United States, telecom operators participate in an auction in the way

network spectrum is allocated. US companies also need to compete with each other in winning customers, which hampers spending on research and development. Chinese companies, however, operate in a different environment, have the capacity to invest in research and development and bear lesser risk of diminishing margins due to competition.

The recent sanctions levied by the US and others against two large Chinese telecommunications firms, has changed the landscape dramatically and in the short term will give opportunities to other companies in this area.

What will it mean to your business?

Already, the major consumer electronic companies are preparing to react to the expected cost of tariffs, including through price adjustments, and tech start-ups will be forced to follow suit. In order to off-set the future expected impact of the tariffs, electronics manufacturers are looking to move production sites out of China to other (low-cost) jurisdictions such as Vietnam, Malaysia and Mexico. We have already seen many companies move their supply chains in that direction, especially the assembly and manufacture of less complex products. As a result, they have been forced to rethink their entire supply chains. Companies should specifically consider adjustments to multi-layer contracts, force majeure clauses, hardship clauses, cancellation and re-issuing rights, minimum volume requirements, and there should be a clear process for handling disputes and contingencies. Human rights, labor, tax and environmental laws also need to be considered as well as product classification and country of origin requirements. Every business affected by the trade war should prepare its own risk analysis and be ready to adjust its strategy as the trade conflict develops.

Moving towards a closed-loop supply chain

In response to a growing world population, scarcity of resources, shorter product lifecycles of electronic devices, and a steadily growing volume of electronic waste, TMT businesses are moving away from a linear model towards a circular economy model (or closed-loop supply chain). The linear model can be described as the "take-make-dispose" model which does not include a process for recycling or re-using products once disposed of. There is now growing consensus that this model is unsustainable and will result in trillion-dollar losses. The closed-loop model, by way of contrast, relies on waste as the primary input for new product creation. It feeds back recycled materials into the production process and "designs waste out of the system". There are many examples of major consumer electronic companies in the TMT sector now moving towards a circular economy model by taking back old devices and designing future products so as to minimize the use of materials. Committing to smart material choices and using closed-loop plastics is another example being adopted. One household name internet search and services company is using circular economy principles in the lifecycle management of the hardware in its data centers, which is reported as having gained 3.5 times the computing power out of the same amount of electricity over the past five years.

What does it mean to your business?

The circular economy is a change of mindset where the focus moves from effective production and cost cutting to a reuse of resources. If done the right way, it can be a win/win for companies, where the disposals are reused and the growth in profit comes from using fewer resources and utilizing smarter production. It will lead to a different way of thinking that takes into account the whole life of a product rather than just from sourcing to market. It is obvious that consumers value this and that this more environmentally friendly production loop will be increasingly scrutinized by consumers in the future. The circular economy will also mean that consumer behaviors will change. We have already seen this in some areas with car sharing pools for example, but most likely this will expand to render the ownership of products almost meaningless. It will simply be important to have access to the product when needed. All of this will make companies rethink their strategies and better understand the changes in customer demand.



Mattias Hedwall

Partner

Stockholm

mattias.hedwall@bakermckenzie.com

Regulating telecoms, ISPs, OTT and beyond

The 5G roll-out will progress and many countries around the world are expected to take steps to facilitate a prompt and coordinated transition to 5G networks. A key challenge to master will lie in finding the right level of regulatory intervention. Just as noteworthy is **access to information held or carried by OTT communications providers** for the purposes of national security and law enforcement. In their fight against crime and terrorism, we expect lawmakers around the world to look at developing access schemes as these have recently been introduced in the UK and Australia. Further, **net neutrality** will continue to be a core legal and political issue in the US, and 2019 will likely be marked by different approaches between the EU and US.

5G roll-out and EU Electronic Communications Code

The development of the fifth generation of cellular mobile communication network has long been an area of particular interest for the EU. Way back in 2016, the EU laid down the basis for the prompt implementation of 5G networks in Europe, issuing the 5G for Europe Action Plan. Such plan contains a number of actions concerning the implementation of 5G directed to Member States and it is tightly connected to the new European Electronic Communications Code, recently enacted by the EU. Its provisions aim to provide operators with investment certainty and ensure coordination of radio spectrum assignments across the EU.

The fifth generation mobile communication network

According to recent studies, 5G will allow a data transfer rate up to 100 times faster, strongly reduce latency (close to zero — below one millisecond), ensure a sharp increase in the volume of mobile data and enable networks to manage one million devices in one square kilometer.

This technology will also foster the implementation of adjacent technologies. For instance, edge computing (which de-centralizes data processing to the edge of the network, thereby reducing latency and increasing speed) will become increasingly more widespread; IoT-related applications will be commercially launched even more from 2019 onward; and dedicated standards will become available alongside the introduction of new applications and use cases such as URLLC (ultra-reliable low latency communications), eMBB (enhanced mobile broadband), or mMTC (massive machine type communications).

In terms of coverage, 5G is expected to reach more than 40% of the global population with 1.5 billion subscribers by the end of 2024.

Recent studies also show that since 2013 the number of devices connected to the mobile cellular network have grown at an annual rate of 33%, and that total worldwide mobile data traffic is expected to reach 136 exabytes (that is 19 gigabytes) per month. The same studies indicate that 5G will enable multiple applications across

industries, including enhanced mobile broadband, the automotive industry, manufacturing, energy and utilities, healthcare and network technologies. The implementation of a network capable of processing large amounts of data has therefore become of crucial importance for the communications sector. Accordingly, 5G has been globally identified as a game changer, and each country has started to get ready for the next technological transformation.

Europe is taking steps to facilitate the deployment of this technology as 5G will be introduced around the world due to high demand for high-speed connectivity services related to certain network characteristics (e.g., a less capillary coverage in terms of radio antennas)

As in any other region, in Europe the transition from the current generation of mobile communication network to 5G may be possible only if supported by an adequate regulatory framework, including the definition of common standards, and appropriate investments, both public and private. Besides, a lack of clear regulation and adequate investments in infrastructures may discourage private investments, as stakeholders may judge investments in the telecoms sector excessively risky. For these reasons, the EU launched a number of regulatory and investments-related initiatives aimed at ensuring a seamless implementation of 5G.

In 2013, the EU Commission backed the 5G-PPP (5G Public-Private-Partnership) project, which is now at its third stage of implementation, focusing on on-field 5G trials. Such project was

also joined by 5G-IA (5G Infrastructure Association), an international association representing industry associations and other stakeholders, which made possible testing a number of applications under 5G networks. Most of the tests conducted during and before 2018 covered the media and entertainment, automotive and transport sectors.

The milestone of the 5G implementation throughout Europe is, however, the 5G for Europe Action Plan ("EU 5G Plan"). The plan coordinates the actions to be taken in-country by each Member State. Indeed, the EU 5G Plan provides a common roadmap for the achievement of certain targets by EU Member States, i.e., (i) the identification of the pioneer bands to be used for 5G by the end of 2016; and (ii) the launch of pre-commercial and commercial services, by the end of 2018 and 2020, respectively.

To date, the EU and most Member States have met the deadlines of the EU 5G Plan. The Radio Spectrum Policy Group ("RSPG") — the advisory group assisting the EU Commission at strategic level on radio spectrum policies — has identified 700 MHz, 3.4-3.8 GHz, and 24.25-27.5 GHz bands as pioneer bands for 5G deployment. Moreover 23 Member States have conducted a total of 139 specific trials related to 5G.

The new European Electronic Communications Code and frequency assignments

The European Electronic Communications Code ("EECC"), enacted through Directive 2018/1972 and to be implemented into national law by each Member State by 21 December 2020, amends the current EU telecommunications legal framework, also with the aim of promoting investments, competition and consumer data protection, with a particular focus on fixed and mobile broadband services.

To ensure timely implementation of 5G across the EU, the EECC contains specific provisions on 5G. In particular, Member States are required to make available the 3.4-3.8 GHz and 24.25-27.5 GHz bands for 5G use by 31 December 2020 with a minimum 20-year license to each company that has been awarded with specific spectrum bands, in order to promote certainty and predictability of return on investment. The EECC also creates a voluntarily peer review process to ensure the consistent assignment of frequency bands across the EU.

Bringing forward the deadline established at EU level, some countries have already made available and assigned to telecoms operators frequency bands identified as pioneer by the RSPG. These countries include: Finland, France, Germany, Ireland, Italy, Spain, Sweden, Latvia and the UK.

Amongst such countries, Italy is the first country in Europe that awarded all pioneer frequency bands, and it is the second worldwide to have auctioned 1 GHz of the 26 GHz band, preceded only by South Korea.

Conclusions

The EU is striving to ensure a prompt and coordinated transition to 5G networks across the region. In this context, the EECC is another crucial step in the pursuit of such target. Besides efforts at EU-level, Member States still need to follow through with the practical implementation of the EECC and EU policies and regulation in the years ahead. In doing so, regulators and policy-makers should carefully evaluate the possible impact of the envisaged regulatory intervention. Indeed, while the adoption of certain measures appears crucial for international coordination and to ensure adequate market conditions, the adoption of an excessive number of rules may hinder investment decisions and drive up operator costs to the detriment of innovation. From another standpoint, regulations may have a significant impact on competition: the possible imposition of excessively burdensome rules on industries which are not impacted by clear market failures may result in distortive effects and hinder innovation. Against this background, regulators should determine the measures to be adopted in an effort to minimize the risk of "over-regulating" the market. With the right balance and correct approach towards innovation throughout the EU, 5G will shortly be a reality across the continent.



Raffaele Giarda

Partner
Rome
raffaele.giarda@bakermckenzie.com



Jacopo Liotta

Associate
Rome
jacopo.liotta@bakermckenzie.com



Andrea Mezzetti

Counsel
Rome
andrea.mezzetti@bakermckenzie.com

Access to data — a new era for national security and law enforcement

The struggle by law makers to keep up with technological change is entering a new phase as governments legislate to give national security agencies and police forces access to the data held by online service providers and associated equipment manufacturers. Whereas traditional interception laws allow access to communications and information managed by telcos, the new laws are focused on access to information associated with a broad range of over-the-top communications providers.

Before the launch of the smartphone, most messages were carried by the public switched telephone network or by traditional email supported by telcos and ISPs. National security and law enforcement agencies were able to intercept messages in transit or access stored messages using powers imposed on telecommunications providers. The touchscreen mobile phone and increased adoption of cloud-based messaging services has placed an increasingly substantial proportion of communications beyond the practical reach of these laws. A government agency may be able to get access to the data carried by a telco, but identifying the relevant communication and rendering it in a comprehensible form is often impossible or impractical.

In 2016, the UK introduced a comprehensive new regime to give national security and law enforcement agencies access to metadata and devices by passing the Investigatory Powers Act 2016 ("IP Act"). The Australian Telecommunications and other Legislation (assistance and access) Act 2018 ("TLAA Act") became law on 8 December 2018.

The new laws go beyond the safe and familiar ground of traditional telecommunications interception and raise issues that will be relevant around the world as other legislatures consider the introduction of similar laws.

The difference between content and metadata in the context of a request for assistance

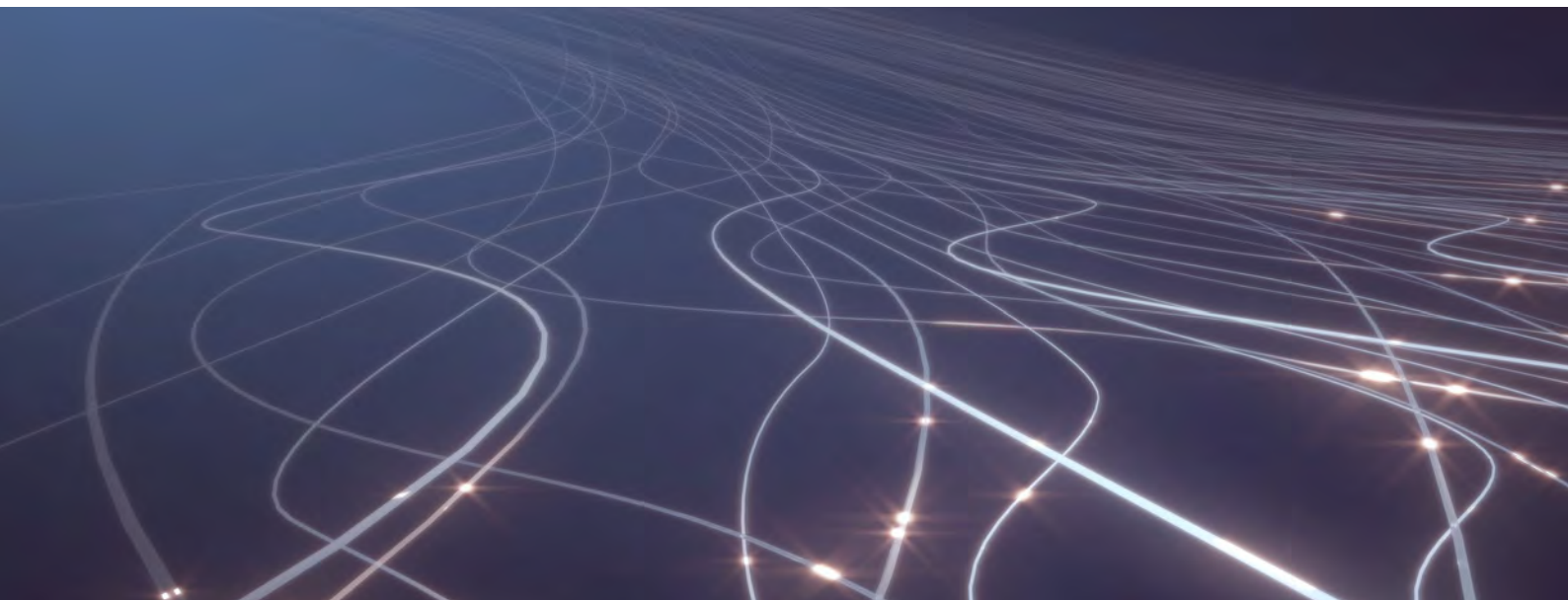
In Australia, government agencies must obtain a warrant from a judicial officer in order to intercept the content of a message or access

a stored message. In the UK, warrants are issued by the executive government and, under recent changes introduced by the IP Act, are now subject to prior judicial review. The requirement for a warrant reflects the sensitivity of accessing private messages as an invasion of privacy and serves to ensure that the security of telecommunications systems is compromised only when strictly necessary.

Metadata is information arising from use of a system and is regarded as less sensitive even though items of metadata — such as name, device, location, to whom you are talking and for how long — can over time reveal substantially more than the content of any particular message. In Australia, government agencies can access metadata when considered necessary without an order from a judicial officer. In the UK, the IP Act has recently been amended to introduce judicial approval for most requests for metadata, following an adverse decision from the European Court of Justice.

In both Australia and the UK, telcos are subject to a regulatory regime that requires them to provide reasonable assistance to law enforcement agencies. These broad obligations are surprisingly powerful. In Australia, requests for assistance are used to request the blocking of unlawful web content and provide the basis on which metadata is made available.

Under the TLAA Act, a very wide range of over-the-top communications providers ("OTT communications providers") — such as businesses that write, install and support software, the manufacturers of device components and facility operators, etc. — can be required to deliver specific assistance to law enforcement agencies, including removing security or getting in before security



systems operate, providing technical information, installing, maintaining, testing or using software or equipment, and making sure information delivered from their systems is in a particular format. These powers can be used at the discretion of the relevant law enforcement agency and could be enforced in association with an official authorization to require the delivery of metadata by OTT communications providers. Under the IP Act, the concept of a "telecommunication service" has been drafted intentionally broad, to cover OTT communication providers, as well as applications and websites that simply provide a messaging service incidental to their main business offering. Operators of telecommunication services can be asked to provide access to communications content, retain and provide access to metadata, enable interference with "equipment" and build a "technical capability" to assist law enforcement agencies.

In Australia, both civil rights advocates and OTT communications providers have opposed the issue of orders requiring assistance without a judicial order.

The implications of sharing security architecture

The TLAA Act enables law enforcement agencies to obtain technical information by issue of a formal request without the issue of a judicial order. Under the IP Act most warrant and notice procedures now require prior approval by a Judicial Commissioner, including "technical capability" notices. These powers might be used to help develop software or equipment that could be installed with the service provider to facilitate access to the provider's systems. It could also be used to identify service providers involved in the delivery of a part of the system so that the law enforcement agency can select a target for a technical intervention or delivery of a warrant.

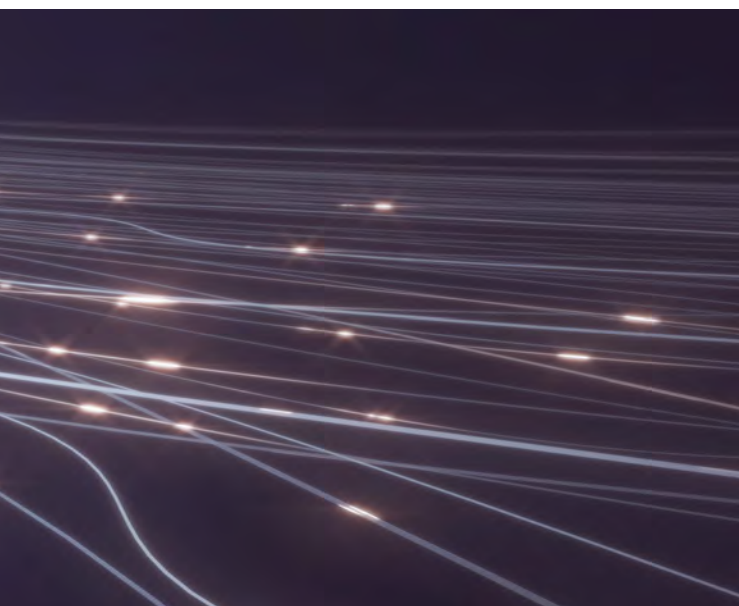
Industry participants have expressed concern regarding the implications of the broad power to obtain technical information. If a government agency fails to keep critical security architecture information secure or develops software or a methodology to circumvent security or encryption, how can the provider ensure that the software or methodology does not become known to third parties and/or is not used for some unauthorized purpose?

The implications of third party software or equipment

The TLAA Act gives a law enforcement agency a discretionary power to require an OTT communications provider to install software or equipment within its systems when, for example, it is considered to be in the interests of national security whether or not a particular investigation is underway. In comparison, under UK law, an intercept warrant may require the installation of equipment to carry out the interception, but this would be specific to an investigation and removed when the warrant expires. Any ongoing technical capability would be implemented by the providers themselves, although the government can dictate the standards that such capability must meet.

Despite lobbying from industry, in Australia the power created by the TLAA Act stands on its own within a traditional regulatory framework giving rise to a range of questions and potential implications:

- Will the software or equipment enable law enforcement agencies to access content or metadata without obtaining a warrant or making a formal request under existing regulations?
- Will the software or equipment give law enforcement agencies unregulated control of a system or parts of the system? The existing regulatory framework does not regulate or even contemplate the possibility of this kind of intervention.



- Software or equipment installed could have data collection, transmission or control functionality that is not known to the relevant service provider and therefore might have adverse consequences for system reliability and performance. There is no obligation under the regulatory framework for an explanation or disclosure of this kind.

The need for extra territorial powers

Key technical information, device manufacture and information infrastructure used to provide or support OTT communications can be located anywhere in the world. The jurisdictional trigger for the application of the IP Act is the provision of telecommunication services in the UK, not whether UK citizens are harmed. Australian law applies more widely to services with one or more end-users and covers equipment to be used or likely to be used in Australia.

In the case of the TLAA Act, law enforcement agencies have the power to issue compulsory notices to entities operating in Australia and entities providing services, facilities, devices, equipment or components for use or likely to be used in Australia. Interestingly, the expanded warrants regime associated with the TLAA Act expressly accommodates the use of the Mutual Legal Assistance Treaty regime where a warrant might be sought against an entity located in a foreign jurisdiction. However, notices requiring assistance and access can be issued against entities located anywhere in the world if they satisfy the criteria.

It might be argued that having the ability to issue notices to entities no matter where located in the world makes the new laws jurisdiction agnostic and therefore would not encourage service providers to locate elements of IT infrastructure away from their aggressive new national security and law enforcement regime. On

the other hand, there is no apparent mechanism for enforcing a notice issued against a party that has no assets within a jurisdiction. Also, even where service providers would be inclined to cooperate with a law enforcement agency in the interests of law enforcement, having the option to negotiate on the basis that government has no mechanism for enforcement would tend to encourage service providers to locate infrastructure outside the jurisdiction.

The extraterritoriality of the new powers gives risk to conflict of laws issues. Within the jurisdiction of an offshore OTT communications provider, laws requiring that information be kept secure are likely to be expressed to permit compliance with lawful orders of government but not a foreign government. The IP Act specifically provides for a conflict of laws defense for a service provider located outside the UK if a law enforcement agency was to try to enforce a duty to provide reasonable assistance. The TLAA provides a defense for failing to comply with an order if it requires an act in a foreign jurisdiction and that act is unlawful in the place it will be carried out.

Conclusion

Access to the information held or carried by OTT communications providers for the purposes of national security and law enforcement is an increasingly important part of the fight against crime and terrorism. Legislative change in this area requires a delicate balance between providing government agencies with the powers they need, protecting the information, systems and customers of service providers and protecting the rights of individuals. The UK and Australian laws highlight the challenges faced by lawmakers looking to develop similar schemes for the protection of their citizens.



Patrick Fair
Partner
Sydney
patrick.fair@bakermckenzie.com



Ian Walden
Consultant
London
ian.walden@bakermckenzie.com

Net neutrality - where are we heading?

Net neutrality is the principle that those who provide access to the internet ("ISPs"), whether by fixed line or wireless technology, must ensure equal access to all content and applications regardless of the source, and without favoring or blocking particular products or websites. This term was first used in the early 2000s - before this point, the technical architecture of the internet had hindered any movement towards preferential routing. However, with technological advances giving ISPs opportunities to differentiate (and implement differential pricing) between websites, users, applications etc., net neutrality has become a question of political policy.

Over the years, ISPs have increasingly begun to use technologies designed to manage traffic across networks. Technologies such as deep packet inspection have allowed for traffic-management techniques whereby ISPs may limit user access to content through download rates, or even block certain sites or services. Such action has been faced with strong opposition, particularly where it has been justified on grounds which are not of a purely technological nature.

Proponents of net neutrality argue that these types of restrictions on an individual's access to the internet stymie innovation whilst ISPs argue that such practices generate the capital needed for greater and more rapid infrastructure investment, which they argue is essential in light of the exponential rise in bandwidth-usage resulting particularly from the growth of online-streaming.

The legal landscape in the EU and the US

The principle of net neutrality was brought into EU law in November 2015 through the Regulation on Open Internet Access ((EU) 2015/2120) (the "Regulation"), which was introduced in addition to the transparency measures outlined in the Universal Service Directive (2002/22/EC). The Regulation aims to ensure all EU users have access to online content and services without discrimination

or interference. It states that in the open internet, all traffic must be treated equally, subject to strict public interest exceptions. The Body of European Regulators for Electronic Communications has since published guidelines which strive to ensure the consistent application of the Regulation across EU Member States. Whilst net neutrality legislation in the EU does also exist at a national level, it is worth noting that grey areas remain. For example, "zero-rating" practices are increasingly employed by various mobile network providers across the EU, which allows for data from preferred providers to be delivered to a user without it counting towards the user's data allowance (e.g., cellular plans sold with uncapped streaming from particular platforms). Many European regulators are yet to fully consider the issue of net neutrality and zero-rated services in light of the Regulations and this consideration may well feature in 2019.

The US has experienced a more tumultuous and higher profile net neutrality journey. With a less competitive market for internet service provision, net neutrality has been an even more contentious debate than in the EU. In 2015, the Federal Communications Commission ("FCC") put in place strong net neutrality rules. However, in December 2017 the FCC under the Trump administration voted to repeal these rules in a drive for deregulation. The repeal has marked a significant shift in the oversight of the internet and enforcement



landscape and has sparked controversy and legal battles, with many states introducing net neutrality laws at state level. The direction of net neutrality in the US is uncertain and the battle between its advocates and its opponents is set to continue in 2019.

The future?

As we head into 2019, Brexit is unlikely to significantly impact the current legislative position on net neutrality in the UK. The draft Open Internet Access (Amendment etc.) (EU Exit) Regulations 2018 published by the UK government look to incorporate the existing EU Regulation into UK law following Brexit.

2019 and beyond is likely to be marked instead by the potential divergence of the EU and US approaches to net neutrality. Subject to the outcome of the legal battles around net neutrality in the US, it seems ever more likely that the EU and US approaches to net neutrality will continue to move further away from one another. The political and legal basis behind this movement will have consequences which will resound internationally. With the EU fostering a more even playing field for content and service providers, this will arguably help to encourage competition, providing a valuable-growth opportunity to less established providers whilst also facilitating a push from the EU to take a greater share of the internet value chain. Whilst in the US, if a pay-for-play digital market does emerge, it is possible that there will be further market consolidation (and growth opportunities) for the already established content and service providers. As the US position crystallizes, commentators will be closely monitoring net neutrality developments in 2019 to assess the potentially wide-ranging practical impact that these diverging political and legislative approaches will have on stakeholders.



Steve Holmes

Partner
London
steve.holmes@bakermckenzie.com



Fleur Chenevix-Trench

Associate
London
fleur.chenevix-trench@bakermckenzie.com

The transactional landscape

M&A activity in tech and telecoms sector was strong in 2018 and we expect this trend to continue in 2019. The cutting edge and exponential growth nature of technology will mean that the sector continues to be on a high and result in a major uptick in the number of well-structured deals being completed. In the **media industry**, changes over the past decade in the way that content is produced, distributed and accessed have led to a wave of consolidation over the previous 24 months and these are set to continue as media businesses adapt to disruption.

Deal activity in TMT

Mergers and Acquisitions activity in tech and telecoms rose to US\$439 billion in 2018 as transformations within the sector continued and the emergence of disruptive cloud, mobile, social and big data analytics technologies drove deal making. The sector had an exciting and strong year for M&A, up 21% from 2017. Megadeals have dominated the headlines.

According to our Global Transactions Forecast, issued with Oxford Economics, big-ticket transactions set for completion in 2019, and favourable market trends are expected to increase M&A activity, with deal values predicted to increase a further 4% to USD 457 billion.

GLOBAL: M&A TRANSACTIONS BY SECTOR (USD BILLION)							
	2015	2016	2017	2018 (F)	2019 (F)	2020 (F)	2021 (F)
Tech and telecom	624	639	364	439	457	397	505

IPO value in tech and telecoms rose to USD 68 billion in 2018, compared to USD 21 billion in 2017, boosted by large listings as well as activities relating to spin-offs from the big tech players. Chinese tech start-ups also continued to look at the US for better fundraising options.

GLOBAL: IPO PROCEEDS BY SECTOR (US\$BN)							
	2015	2016	2017	2018 (F)	2019 (F)	2020 (F)	2021 (F)
Tech and telecom	29	12	21	68	61	29	47

A growing market

Changing business models, expansion of the giant tech players, new and more nimble competition and emerging technologies, such as AI and 5G platforms, are driving activities. With all the signs pointing to a market that will continue to grow, success in the sector will likely involve significant convergence of M&A and transactional activities.

Some transactions have been driven by traditional TMT M&A trends, such as the need for scale and competition for best-in-class technology, talent and content; however activity in new tech is booming, with a wider range of buyers aiming to innovate through acquisition and as acquirers seek global expansion.

“Despite the challenges facing the sector, businesses in all industries are increasingly looking to technology to change the way they do business and propel them in their markets. As the convergence of media and technology, direct-to-consumer capabilities, the cross-sector acquisition of technology, and the expanding demand for data and AI continue, deal making in tech and telecoms will remain buoyant in 2019.”

Michael DeFranco | Baker McKenzie's Global M&A Chair

For technology, AI is going to be hugely active as machine learning and cloud-based services drive demand. Software companies will also continue to seek acquisitions that will allow them to sell suite solutions across multiple functional verticals. For telecoms, 5G networks will play a crucial role and we have already seen forward looking alliances in media.

Mobility and e-commerce

Elsewhere, mobility and e-commerce are continuing to drive activity. In the automotive sector, triggered by the increased adoption of autonomous technology in vehicles, there has been significant investment with key partners getting together to co-invest to bring profitability to the sector. In the consumer goods and retail sector, we also expect to see big increases in M&A activity over the next year with the continued disruption of traditional retail models driving further acquisitions to build ecommerce and omnichannel capabilities.

Consolidation and convergence going forward will continue to be the name of the game as electronic communications and technology set the scene in the transportation and e-commerce ecosystems.

Regulatory and data privacy challenges

Despite the dynamic and exciting market developments, growth in tech and telecoms has been somewhat more muted than anticipated, reflecting an increase in regulatory scrutiny, particularly regarding major deals in the microchip sector that have been looked at by regulators, adding an overlay of market concern around significant market power.

In case of a change of control (in the broadest sense), governmental scrutiny to protect “strategic assets” – such as those in the telecoms, energy, transportation and defence industries – might affect

“The consumer and e-commerce sector will also see big increases in M&A activity in 2019 compared to 2018, particularly as economic stability directly impacts consumer spending ability.”

Roel Meers | Partner, Baker McKenzie



Michael DeFranco
Partner
Chicago
michael.defranco@bakermckenzie.com



Roberto Grane
Partner
Buenos Aires
roberto.grane@bakermckenzie.com



Roel Meers
Partner
Brussels
roel.meers@bakermckenzie.com



Howard Wu
Partner
Shanghai
howard.wu@bakermckenzie.com

“Transactions during the last year in Argentina have been focused on infrastructure investment, including towers and comparable structures that can increase the reach of signals and services. 5G will require new investments and all developments in technology and telecoms rely on infrastructure availability, which in many jurisdictions is of a very low quality. We believe this trend will increase during 2019.”

Roberto Grane | Partner, Baker McKenzie

technology and telecoms transactions, especially along certain trajectories such as Chinese investment into the US. The extended powers of State bodies could therefore affect the transactional landscape. And this not only in the United States (especially with the recent legislative developments around CFUS’ role and jurisdictions), but also in the EU with increased focus on Chinese investments.

Data privacy is also expected to have impact on M&A activity in the next 12 months, particularly with the introduction of the European Union’s General Data Protection Regulation and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) trade agreement, and data increasingly seen as a key asset.

A global outlook

The US and Europe will play major roles in deal making in 2019, with China more than likely at the forefront of activity, especially as it is already looking at new and sophisticated technologies such as 6G. In Asia, the vivacious atmosphere and environment create excellent conditions for transactional opportunities. Africa will also be a region for significant potential in the tech space.

With all the signs pointing to a market that will grow rapidly in 2019, the cutting edge and exponential growth nature of technology will mean that the sector will continue to be on a high, enjoying a period of substantial activity that will result in a major uptick in the number of well-structured deals being completed, with the sector concurrently exhibiting no obvious signs of being curtailed.

Content media: the transactional landscape

A brave new world

The last decade has seen a sea change in the way that consumers access content. This shift is most stark in the television and music industries — a decade ago television was dominated by linear national broadcasters and the CD remained the most popular music format.

The emergence in recent years of subscription based "over the top" (OTT) original content has challenged the position of linear broadcasters and traditional production houses, as cable customers continue to cord cut and shave. In the music industry, user numbers for music streaming platforms have grown exponentially over the past decade, leading to record labels re-evaluating their business models for a digital era and the declining fortunes of retail and digital music stores.

These changes to the production and consumption of content have led to a wave of consolidation over the previous 24 months and are set to continue as businesses adapt to disruption.

Content is king

Recent consolidation in television and film has been both horizontal (e.g., consolidation amongst production studios) and vertical, with production studios being acquired by broadcasters and telecommunications companies. One rationale for the spate of studio acquisitions is to bolster a buyer's content catalogue, paving the way for the launch of new direct-to-consumer services to challenge the position of established OTT platforms.

As the direct-to-consumer content race heats up, we expect further transactions in 2019 and ahead as new OTT entrants seek to utilize cash reserves for content acquisitions, in particular film and TV studios in the US and Europe.

The race for the "rest of the world"

We also expect 2019 to feature a number of international consolidation transactions. In Europe, co-operation between national broadcasters is likely — either in the form of acquisitions or joint ventures — to deliver

international content catalogues directly to consumers. We anticipate US bidders will also continue to look at European businesses in an attempt to increase their European footprint.

In the music sector, we expect the race for international audiences — particularly in Latin America and India — to lead to consolidation as the major music streaming platforms seek to increase user numbers outside of their core markets.

Data headwinds

A further strategic benefit of a direct-to-consumer OTT service is the rich dataset it provides, including which demographic is viewing which type of content, how often and where. The collection of such behavioral data by "Big Tech" has been questioned by politicians and there is a risk of regulatory intervention to break up any perceived market dominance.

“Data is key in the digital economy. We must therefore carefully review transactions which lead to the acquisition of important sets of data, including potentially commercially sensitive ones, to ensure they do not restrict competition.”

Margrethe Vestager, European Commissioner for Competition

Regulators are increasingly scrutinizing the risk of vertical consolidation allowing upstream media content producers to collect user trend data in order to influence future production and delivery decisions, giving those providers a competitive advantage over downstream platforms. Any increased regulatory intervention could either inhibit future deal activity or lead to divestments.

Conclusion

Recent years have seen high volumes of deal activity in the media industry, owing to the changing landscape of content consumption. This, together with the more recent desire for user growth in non-core geographies and the increasing risk of regulatory intervention, is likely to see deal activity continue in the sector for the foreseeable future.

Recent and future "mega deals" will also lead to further divestments of non-core business units, either mandated by regulators or as part of integration efforts. Deals to date have been dominated by strategic players rather than private equity, but these divestments should guarantee continued deal activity in the sector and present opportunities for all market participants.



Will Holder

Partner
London

william.holder@bakermckenzie.com



Paolo Galli

Counsel
Milan

paolo.galli@bakermckenzie.com



Dewi Evans

Associate
London

dewi.evans@bakermckenzie.com



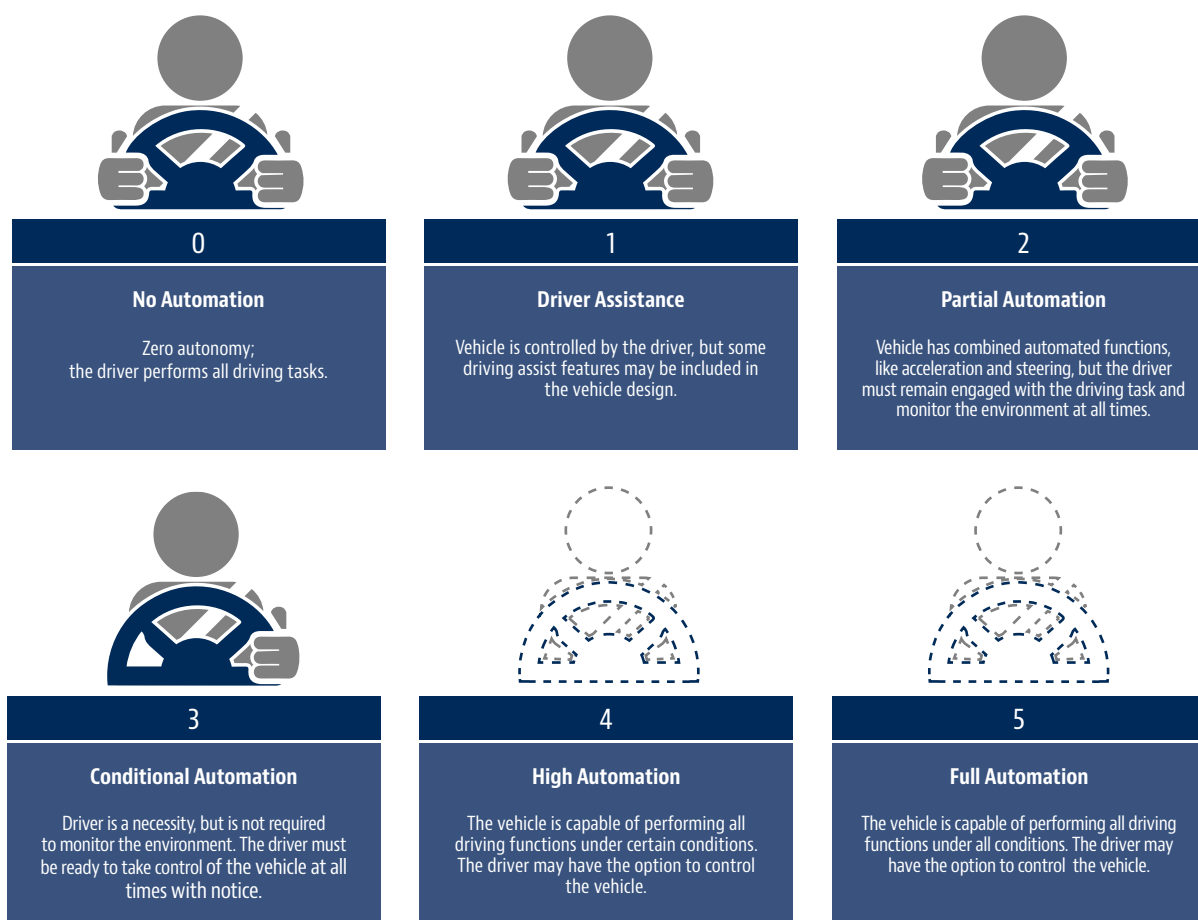
The benefits and challenges of living in an interconnected world

Autonomous vehicles are a prominent illustration of the increasingly interconnected world. They promise various improvements in our day-to-day life and bring together the automotive, technology and telecommunications sectors. As the technology underlying autonomous vehicles is being developed, laws and regulations need to adapt raising complex questions around liability, insurance, access to in-vehicle data and common industry standards just to name a few. This process has been underway for some time, but many questions are unanswered and we expect further debate and some responses in 2019. Given the array of complex technologies embedded in automated vehicles and other IoT devices, common industry standards — and with them **Standard Essential Patents and FRAND licenses** — will continue to rapidly gain importance and businesses will face a challenging patent landscape.

Autonomous vehicles — where are we driving to?

The race to develop and deploy autonomous vehicles — more specifically those that require no human intervention (defined in the Society of Automotive Engineers (SAE) standard as Level 5) — continues to attract billions of dollars of investment from the traditional automotive manufacturers (OEMs), global technology companies and investors. The focus on, and investment in, autonomous vehicles is unsurprising, with the global market for automated vehicles projected to be worth USD 7 trillion dollars in 2050 and expected benefits ranging from improved safety (a computer does not get tired) to more efficient traffic management, better urban planning, increased productivity and social inclusiveness (as those who can no longer afford or are not capable of driving are granted mobility).

SOCIETY OF AUTOMOTIVE ENGINEERS (SAE) AUTOMATION LEVEL



Source: <https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety>

Whilst limited commercial trials of fully autonomous vehicles have begun in countries such as the US, Italy, the UK and China, most analysts predict at least 10 years before fully autonomous vehicles are launched in the market and much later until we see mass adoption on the roads (IHS for example predicting 23 million autonomous vehicles on the roads by 2035). In the meantime, vehicle manufacturers are focused on deploying increasingly sophisticated levels of automation to new models. With parking, lane assistance, distance and speed controls now commonly automated in cars, the next step is conditional automation — where the car can drive itself in certain cases, but the driver must always be on hand to intervene (Level 3, SAE).

Autonomous vehicles are where the automotive sector and the technology and telecommunications sectors intersect and businesses across these sectors collaborate and partner to develop the technology underpinning autonomous vehicles such as: cloud services, fast low latency connection of the vehicle to other vehicles and the required road infrastructure and advanced driving software using AI to make key safety decisions. Key players have already formed strategic partnerships. For example OEMs are typically working with large technology companies, chip manufacturers and other technology investors. Technology companies (and some OEMs) are also working with ride hailing services.

As the technology underlying autonomous vehicles is being developed, laws, regulations and ethical standards need to adapt as well. This process has been underway for some time. We expect governments, lawmakers and regulators to accelerate the process in 2019 and beyond. Below is a selection of key regulatory, intellectual property and data privacy/security issues which are going to make a mark in the year ahead.

Key regulatory issues

Lawmakers and regulators worldwide are starting to develop laws and technical and regulatory standards to facilitate and properly regulate the development, testing and operation of autonomous vehicles. [Baker McKenzie's Global Driverless Survey \(March 2018\)](#) surveyed the progress of regulation across 33 jurisdictions worldwide and found:

- the majority do not yet have specific regulations and rules relating to driverless vehicles
- whilst 12 jurisdictions out of the 33 surveyed have some legislation, regulations or rules that address or apply specifically to driverless vehicles, these are still at an early stage with the majority adapting existing road rules to facilitate testing of partial or fully driverless vehicles in specific circumstances.

Overall, lawmakers and regulators have a long way to go and face complex questions, including:

Industry vs top-down regulation — In developing these new laws what areas will be left to industry-led self-regulation versus top-down government laws?

Adapting or replacing existing road laws — The preferred, faster approach seems to adapt existing rules rather than creating new rules from scratch. If existing rules and regulations are adapted, how do issues such as the definition of "driver" and "control of vehicle" as well as reflecting fundamental changes in vehicle design (removal of steering wheel and pedals) get resolved?

Data privacy and cybersecurity requirements — What security measures will be mandated to protect autonomous vehicles against hacking?

Liability and insurance requirements — As the driver cedes control to the vehicle itself, complex liability issues arise. For example who owes the duty of care — is it the OEM or another third party supplier? How does fault get allocated in an accident if, for example, the driver may have been expected to take control of an autonomous vehicle? What is the best way to insure autonomous vehicles — should the OEM include bundled insurer or the owner/passenger be required to have motor insurance? Some answers to these questions are beginning to emerge in specific jurisdictions.

One example is the UK's Automated and Electric Vehicles Act 2018 which broadly extends the principles of fault based motor insurance to autonomous vehicles. Where a vehicle in self-driving mode is insured, liability will be dealt with under a single insurer model covering the driver both when driving and when the self-driving feature is activated. The Act specifies when liability shifts from a driver to the vehicle manufacturer itself and when insurers will be able to exclude or limit liability to the insured, including prohibited software alterations. However, where the OEM or another third party is liable for the damage (which in itself generates complex evidential issues), the insurer or vehicle owner will be entitled to claim against the manufacturer under existing laws such as product liability.

AI decision making and transparency — The AI software used in autonomous vehicles must be transparent in how critical collision decisions are made to ensure vehicles are trusted by users. A significant amount of work on ethical frameworks underpinning AI decision making is already underway and we are likely to see further important developments in the year ahead.

Protection of Intellectual Property

Given the multiple and complex technologies incorporated in autonomous vehicles, the infrastructure necessary to support them and the collaborative partnerships necessary to develop and implement such technologies, stakeholders will need to ensure adequate IP protection of their inventions.

Patents will remain central to most of the key players (including technology companies and OEMs) which are building large patent portfolios with Bloomberg Law listing more than 6,300 issued patents relating to AV technologies. Care should be taken however in drafting patents describing software inventions, particularly around ML/AI, which usually strives to automate or replicate acts

performed by a human. For example, in the US, implementations in software of abstract ideas without an additional inventive step are patent-ineligible. What constitutes an abstract idea continues to evolve, but broadly the US courts have invalidated patent subject matter that could be performed through an ordinary mental process in the human mind or by a human using pen and paper. Trade secrets may be a viable alternative to patent protection where patent eligibility is an issue but carefully limiting the distribution of trade secret information as well as drafting and enforcing confidentiality restrictions will be critical in this case. The underlying source code itself (but not its functionality) may be protected by copyright.

Given the array of complex technologies involved, there is a need for common industry standards so that automated vehicles will be able to work seamlessly in different countries. As such standards develop and existing ones are implemented in the technology used by autonomous vehicles (e.g., 5G), standards essential patents will be increasingly important in this sector along with questions of what constitutes FRAND (fair reasonable and non-discriminatory) licensing. We therefore view it probable that patent litigation will emerge in the automated vehicles sector.

Autonomous vehicles and data

Due to numerous sensors present in vehicles and integrated into mobility infrastructures, during a two-minute car drive thousands of data points are collected, including information relating to the vehicle, data relating to the driver, location, route and telematics data. The insights that can be derived from this data will change the way various services such as roadside assistance, vehicle insurance, vehicle repair and car rental are provided. Beyond that, the data will have enormous commercial value and industry players with access to the data, such as OEMs and digital platforms, are already facing the challenging task of turning that data into a competitive advantage.

At the same time, there seems to be a growing consensus that such data should be made accessible more broadly to enable fair and effective competition for innovative solutions. However, there is not yet a governance model for making data accessible and views vary widely. Do we need legislation regulating access to in-vehicle data or should access to data be governed by freedom of contracts? In Europe, 2019 will hopefully bring more clarity as the European Commission is expected to issue a recommendation on how to govern access to in-vehicle data following a public consultation which closed in December 2018.

Needless to say that adequate data privacy and security practices should be a business priority, given the complex and multifaceted data processing activities occurring in the context of autonomous vehicles activities. This is the case, for instance, when data is collected and processed in-vehicle, exchanged between vehicles and personal devices connected to it, exchanged between vehicles and external entities (e.g., infrastructure managers, vehicle

manufacturers, insurance companies, car repairers), and broadcast to surrounding vehicles and infrastructure entities. Overall, general data privacy and security laws and regulations govern the processing of car data and the real challenge lies in the practical implementation of the industry-agnostic legal and regulatory requirements. Being transparent around data flows, facilitating data subject control and having a legal basis for processing should be priorities for businesses. In the EU, the European Data Protection Board recently foreshadowed that it will issue Guidelines on Connected Vehicles in 2019/2020, which will provide much-needed guidance. Sector-specific legislation and industry self-regulation might also be forthcoming in some jurisdictions such as is the case in the US already (e.g., the US Self-Drive Act which includes data privacy and security provisions). Sound data privacy and security compliance instilling consumer trust will be crucial for the social adoption and widespread utilization of autonomous vehicles.

Conclusion

From establishing frameworks governing access to, and monetization of, the huge datasets generated by autonomous vehicles, continuing efforts to tackle complex liability issues by adapting existing legislation (and enacting new laws) to important new technology developments, including those in edge computing and AI processors, 2019 and beyond will be an exciting and busy time for those in this sector.



Raffaele Giarda

Partner
Rome
raffaele.giarda@bakermckenzie.com



Anna von Dietze

Senior Knowledge Lawyer
Dusseldorf
anna.vondietze@bakermckenzie.com



Jason Irvine-Geddis

Knowledge Lawyer
Belfast
jason.irvinegeddis@bakermckenzie.com

The growing importance of standard essential patents in times of digitalization

As digitalization transforms traditional companies into tech companies, these firms are now facing new challenges previously confined to tech incumbents. One of these challenges is the patent landscape in the high tech industry. Patent infringement can have a massive impact on the business especially since in important jurisdictions like Europe, the US and China, the standard remedy in case of patent infringement is injunctive relief.

SEPs and FRAND

A special kind of patent that these "new high tech companies" are now facing are standard essential patents ("SEPs"). SEP refers to patents that cover technologies mandated by technical standards (e.g., UMTS, LTE, Wi-Fi, 5G), which standards are issued by standards-setting organizations (SSOs, e.g., ETSI, 3GPP), in order to ensure that products or processes function in a specific manner and are interoperable. Use of technical standards is essential in fields including mobile communication and audio and video encoding. For example, connected cars, smart home devices and robots in high-tech production facilities need to use mobile communication standards. Similarly, media companies running streaming services are necessarily using video coding technologies specified in industry standards. The underlying technology is often subject to numerous SEPs.

What SEPs have in common is that their use is technically and/or economically inevitable. This puts the SEP owners in a privileged position in that others are dependent on being allowed to use an underlying invention in order to manufacture a product. To avoid misuse, SEPs are "FRAND-encumbered", meaning that SSOs require the patentees to promise licensing the SEPs on Fair, Reasonable, and Non-Discriminatory ("FRAND") terms to any third party.

SEP litigation

The importance of standards gives SEPs a special status which in many jurisdictions, such as in Europe, the US and China, often implicates antitrust law issues, such as whether a patentee refusing to comply with FRAND commitments abuses a dominant position in violation of antitrust laws.

The European Court of Justice (ECJ) has ruled that in SEP litigation the infringer can avoid injunctive relief by taking a license which the patentee (due to antitrust law) must grant on FRAND terms. The ECJ has provided guidelines on how to resolve the conflicting aspects between patent and antitrust laws by defining steps that must be met by the SEP holder and the infringer. If the patentee fails to meet these guidelines this will be considered an abuse of a dominant position under Article 102 TFEU, resulting in the prevention of seeking injunctive relief. If, on the other hand, the infringer fails to comply with its obligations an injunction can be granted. Also, Chinese courts have partly adopted these guidelines for assessing whether the SEP holder can seek injunctive relief. However, the interpretation and implementation of the details of these guidelines are subject of ongoing litigation in various countries that involve complex questions of patent and antitrust laws.

When a license agreement is negotiated during infringement litigation, depending on the forum, judges might provide detailed

calculations on which royalty rate they consider FRAND (UK) or just rely on a corridor built by prior license agreements (Germany). However, some courts (in Germany and the UK) consider it FRAND if the patentee requires a worldwide portfolio license. This can trigger complicated questions with regard to the antitrust laws in foreign jurisdictions covered by such license agreement. In such cases, the litigation must be handled from the beginning by a multinational team of attorneys who can handle the global implications of the patent litigation.

Key actions for manufacturers

As SEP litigation is a real threat, companies manufacturing products which implement a technical standard should check with their component suppliers using the standard whether they have taken licenses at least from the most relevant SEP licensors. Furthermore, supply contracts should be reviewed for IPR indemnification clauses. When being approached by a patentee, in order to avoid inadvertently losing the FRAND defense and being faced with an injunction, the user of the patented standard needs to

understand how and in what timeframe they must react in view of the sophisticated case law in the relevant jurisdiction(s). This requires companies implementing standards to undertake careful training of their employees, at least in those jurisdictions that are important (typically where the a product is manufactured and marketed and/or sold).

Moving beyond the telco sector

While in the past these issues have been relevant mainly for telecommunication companies, now the manufacturers of connected devices (such as smart home devices and automated vehicles) are moving into focus. However, in Germany, one of the key forums for such litigation, we also see intense lobbying for facilitating litigation in the field of audio/video codecs. Just recently the German Federal Court of Justice has confirmed that a German patent containing a method claim covering the encoding of a media file is infringed if the coding happened abroad but the file is imported (streamed) to Germany. This will further increase the already high volume of respective litigation.



Alexander Ritter
Senior Associate
Munich
alexander.ritter@bakermckenzie.com

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



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



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

Editors



Anna von Dietze
Senior Knowledge Lawyer
Dusseldorf
anna.vondietze
@bakermckenzie.com



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

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

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

www.bakermckenzie.com

©2019 Baker McKenzie International is a global law firm with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner or equivalent in such a law firm. Similarly, reference to an "office" means an office of any such law firm.

This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.