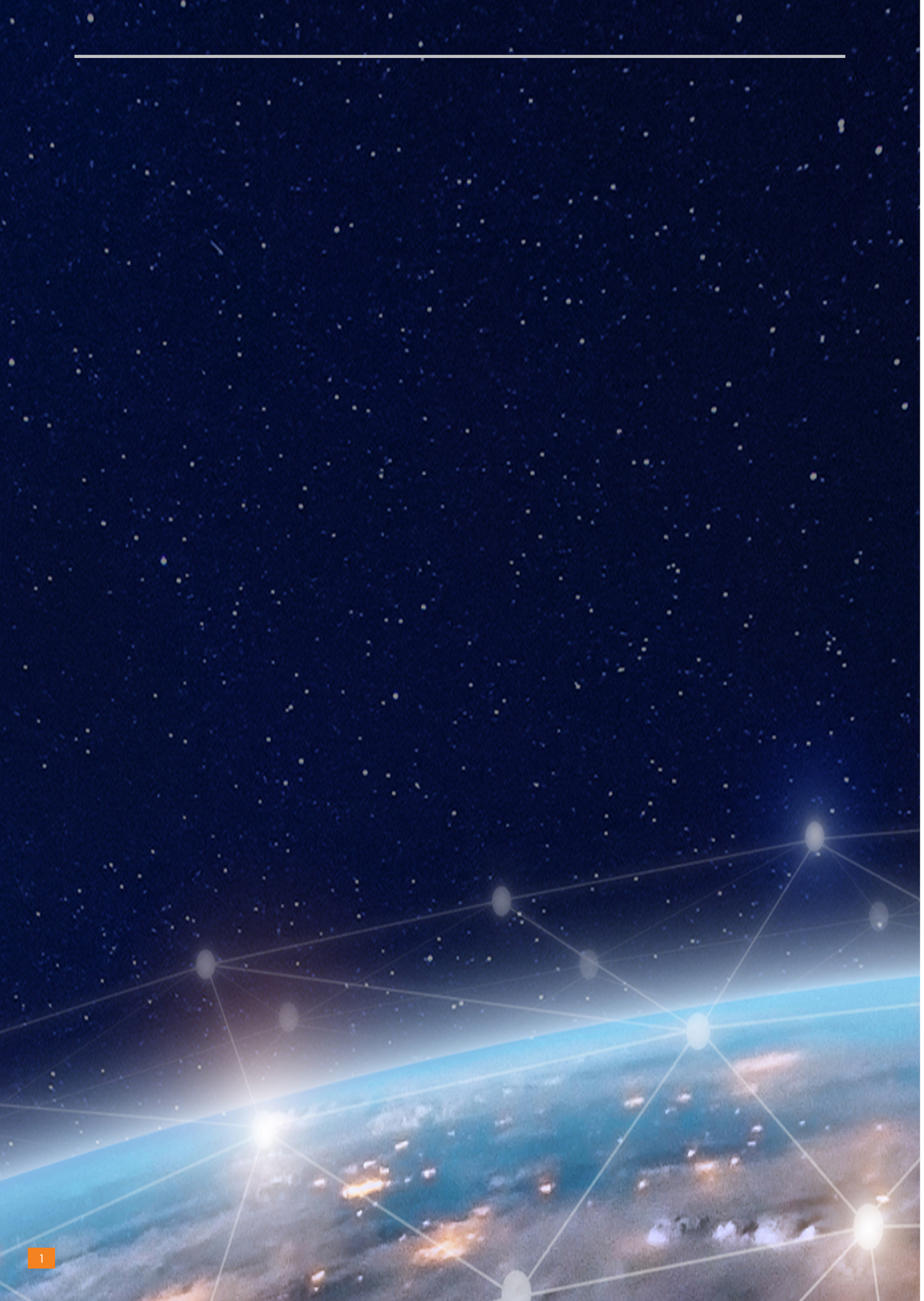
Baker McKenzie.

TECHNOLOGY, MEDIA & TELECOMMUNICATIONS

DATA AS AN ASSET

Key themes across business models and multidisciplinary trends

September 2019



Contents

Data as an Asset - Key themes across business models and multidisciplinary trends

Foreword

Data is an asset. Many of today's successful companies are based on data-driven business models. Big tech businesses are naturally leading the way, but across all sectors businesses are under pressure to leverage or monetize data. Monetizing data can be done in various ways, such as personalizing products or services, making manufacturing or logistic processes more efficient, automating tasks and operations, engaging in targeted advertising and improving internal systems, just to name a few. Possibilities seem limitless and businesses are becoming ever more sophisticated and creative in deriving value from data.

But as data-based or digital business models emerge and evolve around the world in each and every sector, legislators, policy makers, regulators, academics and others - across disciplines - are working out how best to respond to, and regulate, these new business models. The objective is to develop rules that foster socially beneficial innovation, preserve human values, protect consumers and at the same time nurture competition.

The policy discussion has been underway for quite some time now. While some countries are ahead of others and, naturally, local divergences exist, we are seeing similar trends and themes emerging across the globe. Notably, these themes go way beyond the traditional disciplines of data privacy and security regulation, and cut deeply into various areas of law – from competition and antitrust to tax, from M&A to employment, and more. The debate has some way to go before we will see more concrete or specific regulation, but in a world where legislators and regulators are increasingly collaborating and learning from each other as they grapple with the same issues brought about by technological transformation, a global and multidisciplinary perspective is needed in order to see what is coming.

In this publication, we have collated those key themes and trends around data as an asset and driver of economic growth that we expect to have a profound impact on the legal and regulatory landscape, industry standards and, ultimately, business practice.

> "Maximising the value of data assets is at the core of the digitisation of all sectors of the modern economy. We are only at the very start of considering how traditional legal disciplines apply to this new world and where the boundaries of acceptable norms and obligations will lie."
>
> **Adrian Lawrence**

Data as an asset - commercial considerations

Data has been catapulted into the category of top business assets and businesses are rightly looking to protect their data from the competition. But due to the odd nature of data and the complexity of the data value chain with numerous stakeholders contributing to the creation, aggregation, structuring, enrichment or analysis of any given data set, the legal concepts and rules conceived for traditional types of assets cannot be easily applied to data. Trade secrets and contractual arrangements are emerging as the most effective ways to protect one's data from being inappropriately accessed or used by others - though they are not without challenges. Another challenge lies in finding the right balance between protecting ones data and opening it up as part of commercially beneficial data sharing initiatives.

Taxing the digital economy: the role of data

As much as businesses are working out how to derive value from data, governments are grappling with how to tax the value attached to that data. Diverging approaches are emerging across the world and as any tax imposed on the value created through data ultimately reduces the value of that data for the business, the emerging schools of thought deserve close attention, even at this early stage, to enable businesses to plan effectively.

Data compliance in the data economy - an ongoing balancing act

Without question, the importance of complying with data privacy and security regulation increases with the growing collection, use and value attached to data. Around the world, countries are introducing or reforming comprehensive data privacy and security regimes resulting in a constantly evolving compliance landscape. In addition, regulators are becoming tougher on businesses with non-compliant data management practices, and fines are increasing to levels that hurt. While data compliance is paramount from a risk management perspective, businesses are increasingly turning good data management practices into a competitive advantage.

Big data and antitrust

As data has become a valuable asset, it is high on the agenda of competition authorities as they consider whether existing antitrust rules and procedures remain fit for purpose. Data is not their only concern, but it is at the heart of the digital economy and features prominently in various "digital antitrust" reports issued around the world. A common concern is that the economies of scale and scope associated with some data holdings can create a barrier to competition, giving companies with the most comprehensive, well-curated and recent data a powerful advantage. Regulatory responses are still evolving, but proposals range from appointing a digital regulator to recommending privacy law changes, from promoting data portability to - in the extreme - mandating data access. It is a vivid debate that has still some way to go.

Open data and one of the first use cases: banking

The concept of open data is gaining traction in the data economy as regulators are increasingly taking the view that those businesses which have access to rich data sets have a competitive advantage over those that do not. One way regulators propose to address this issue of perceived imbalance is to give consumers the right to facilitate, and indeed mandate, the movement of their data around the ecosystem. In other words, consumers (and other businesses) should be able to require those businesses that hold their (personal and non-personal) data to make that data accessible to third parties (subject to strict requirements). As banks hold an abundance of data about their customers by the very nature of the service they provide, but also because of regulatory requirements, they have become the initial use case for open data.

The future of work in the data economy

The digital age is fundamentally changing the way we work. With traditional contracts of employment and offices on the decline, contingent and remote workers increasingly the norm, and digital well-being becoming the subject of legislation, organizations must adapt and evolve.
This includes, for example, finding the right balance between taking advantage of HR analytics while not engaging in inappropriate employee surveillance, allowing the workforce to work flexibly, but promoting healthy digital behavior, and automating processes and tasks while adding new skillsets to the human workforce.

Blockchain – new technologies benefiting from and enabling the data economy

New technology is a key feature of the data economy, with blockchain being a prominent example given that it is, in essence, a new architecture for storing, sharing and elaborating data. While maybe no longer "new", we are still in the exploration phase of identifying the primary use cases for this technology beyond cryptocurrencies. From a regulatory perspective, many regulators are advocating a "technology-neutral" approach to blockchain, holding that blockchain should be viewed through the lens of existing sector-and-issue-specific regulations and that new laws are not required at this time.

New infrastructures - automated and connected vehicles, smart roads and smart infrastructure

Autonomous mobility is a prominent feature of an increasingly interconnected world where the Internet of Things impacts not only vehicles, trains, aircraft, drones or other movable assets, but it also plays a significant role in our cities, our buildings, roads, and supporting infrastructure like airports and ports. As the underlying technology evolves, the challenging task of creating a legal and ethical framework to govern the technology and its various use cases is also underway. Achieving an optimal balance will likely require a combination of top-down regulation and industry-led collaboration with regulators.

Data and disputes

As the value of data increases, we expect the number and complexity of disputes around data to grow. Regulators and courts will come down hard on those that do not take their data safeguarding responsibilities seriously. As the size of fines increases, so does the likelihood of challenges to fines. We anticipate more complex litigation in this area, with supply chain actors and ecosystem partners joined as defendants and seeking reallocation between themselves, security providers directly in the firing line, and insurance coverage in particular being tested on a more regular basis. Moreover, as it remains difficult to assert IP protection over data, there is going to be more pressure on putting trade secret laws to the test to protect this valuable asset. Finally, we will likely continue to see a rise in collective action mechanisms outside the US, and law enforcement and security agency access to data will remain a hot topic.

Deals in the data economy

Technology acquisitions continue to be a driving force for M&A in 2019 and data is playing an increasingly important role. This is reflected throughout the whole deal process, from the due diligence phase, where the data management practices of the target receive much more attention than in the past. In the data economy, data also influences the purchase price which raises the complex question of how to measure or place a value on data.

"Data-driven business models raise a myriad of novel legal issues which cut across various areas of law -- from data privacy & security compliance to antitrust, from tax to corporate law and more. It is compelling to look at how across the globe comparable debates are taking place and how historically distinct legal disciplines are now, more than ever, intersecting in order to adequately respond to such modern industry trends and new business models."

Raffaele Giarda

With a big thank you to all our contributors:

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

Adrian Lawrence
Partner
Sydney
adrian.lawrence@bakermckenzie.com

Data as an asset - commercial considerations

In the data economy, the value that can be derived from data creates tremendous opportunities for businesses of all sizes and businesses are under pressure to remain competitive. Doing so is of course easier said than done. It requires businesses to identify the best use cases for their data, find ways to protect their data as a business asset while increasing its value by sharing it with others, comply with ever evolving and often inconsistent laws and regulations, and meet consumer expectations for responsible and transparent handling of their data.

Data - an odd creature?

While for many years, we have been thinking of data as personal data, in the data economy, the term data is much broader and includes various types of non-personal data (e.g., enterprise data, statistical data, analytical data, transactional data, scientific data, public data, etc.). In fact the distinction between personal and non-personal data is becoming increasingly difficult and is being challenged by those that advocate a more nuanced regulatory model seeing data on a spectrum from closed to shared to open.

Data has been catapulted into the category of top business assets and now enjoys a status similar to that of traditional business assets like real property, physical assets, commodities and intellectual property. However, data is very different in nature to traditional assets in that:

- data is intangible and difficult to attribute value to (cf. physical assets)
- unlike commodities which derive value from scarcity (e.g., gold) or utility (e.g., oil), data is infinite, non-rivalrous, easily reusable and derives value through use and often through combination and sharing
- data is not subject to statutory protection like IP assets (e.g., copyright or patents)

As a result the legal concepts and rules conceived for traditional types of assets cannot be easily applied to data.

Who owns data?

In the data economy, businesses often frame claims, negotiations and controversies regarding data access as one of ownership arguing, for instance, that they have collected, aggregated, analyzed or transformed the data and are therefore the owner of that data. Given the complexity of the data value chain with numerous stakeholders contributing to the creation, aggregation, structuring, enrichment or analysis of any given data set, it is common for various participants to assert ownership rights in one and the same dataset. However, most (if not all) jurisdictions, do not currently recognize an ownership right in data like they do for traditional (tangible and intangible) assets. As a matter of law, individuals do not own data about themselves, nor do businesses own data they collect and process, regardless of the popular narrative or conception in this regard. The key argument against an ownership right in data is the need to ensure the public interest in access to, and reuse of, data and encourage data sharing (rather than locking down data). Overall, the crucial question to ask (and negotiate) is not who owns data but who controls access to, and use of, data to what degree.
Click here for a detailed discussion.

Monetizing data

Data monetization is all about deriving value from data. It is common to differentiate between direct and indirect data monetization.

- Direct data monetization is about generating direct revenue from data by packaging-up and selling or licensing your data (in raw or refined form) to third parties that will use it for their own purposes. Direct monetisation can also include trading data with other organizations.
- Indirect data monetization is focused on making information ccessible and deriving insights from that information in order to, for example, improve processes, increase customer engagement, predict trends, analyze performance, or develop new products or services, either for your own business or for your customers.

How is my data protected as a business asset?

Given its commercial value, businesses are rightly looking to protect their data from the competition much like they protect a patent or trademark. But due to the odd nature of data, traditional IP protections such as copyright or patent law, the law of confidence, or database rights only provide very limited protection (if any). Trade secrets and contractual arrangements are emerging as the most effective ways to protect one's data from being inappropriately accessed or used by others - though even they are not without their challenges.

Trade secrets

Trade secrets are unregistered rights and protect, in principle, any information that belongs to a business, which is secret (i.e., not known or readily accessible), has economic value because of its secrecy, and is subject to reasonable steps to be kept secret. The overall objective of trade secret protection is to protect businesses from unfair misappropriation of commercially valuable confidential information. Trade secrets can include a vast array of information, including ideas, processes, product creation, recipes, methodology, plans,
software and data.

As trade secrets are granted special protection based on the nature of the information (valuable and secret) and the way they are treated by their owners, in order to be able to rely on trade secrets protection, it is essential to proactively manage one's trade secrets Click here or our checklist for protecting trade secrets.
For businesses that want to rely on trade secrets in order to safeguard their data from third party access or use, it is paramount to protect the data from disclosure and tightly control access to the data through appropriate security measures and processes. However, this does not sit easily with the proposition that data derives value through use and often through combination and sharing which, in practice, increasingly leads to various stakeholders generating and accessing shared data sets. So, a major challenge lies in finding the right balance between sharing data for value creation and locking down data in order to benefit from trade secret protection. Given this dichotomy and the fact that trade secret laws around the world are relatively new and untested, it remains to be seen whether they are the optimal basis for protecting data as an asset.

Contractual arrangements

In the absence of reliable statutory protection of data as an asset, businesses are resorting to contracts to agree rules of data governance. Parties can, in both a B2B and B2C context, agree between themselves rules for access to, and storage of, data; rights and limitations regarding the use, aggregation and sharing of data; pricing; termination rights and processes (including requirements to return data upon termination); representations, warranties and indemnities; allocation of liability, and various other governing rules.

So, in some way, contracts enable businesses to control access to, and usage of, "their" data by imposing the conditions for such access and use. However, there are important limitations. Firstly, anticipating the parties' needs, use cases and risks with respect to relevant data and adequately agreeing in advance the respective rights, obligations and risk allocations seems almost impossible in the complex data value chain. Secondly, those contracts only bind the contracting parties and cannot be enforced vis-à-vis third parties. And thirdly any such contractual arrangement will need to comply with applicable regulation (e.g., data privacy and security obligations).

Data sharing

There is a clear trend in many jurisdictions towards incentivizing data sharing and making previously tightly held data accessible more broadly - often within an industry ecosystem - in the name of innovation, competition and consumer control.

Sharing of data may take different forms, such as the reciprocal exchange of data, one or more organizations providing data to one or more third parties, organizations pooling information and making it available to each other or third parties (e.g., as part of industry data sharing initiatives), the opening-up of government-controlled data sets, or one-off disclosures of data.

- For instance, in the automotive sector, car manufacturers and service providers have already started initiatives for sharing real-time anonymized data for safety purposes. Or, in Europe, under PSD2 banks are required to share some of their customer data with third parties at the request of the customer and subject to strict conditions (see chapter on Open Banking).
- Australia is introducing a consumer-driven data portability regime in the form of a "consumer data right" intended to improve consumers' ability to compare and switch between products and services by facilitating the movement of their data around the ecosystem. Currently the consumer data right provides for data portability in the banking sector (much like PSD2 in Europe), but there are plans to broaden its scope to the energy and telecommunications sectors, and ultimately across the entire economy.
- Competition regulators are also actively promoting data sharing and data portability as they increasingly argue that those businesses with access to rich data sets have a competitive advantage over those that do not. Proposals on the table range from data portability regimes to mandating data access in certain circumstances by way of sector-specific regulation. But while they generally see benefits for competition and consumers in data sharing and data pooling arrangements, competition regulators are also cautioning that such arrangements can become anti-competitive in some situations and demand a considered and tailored approach.

However, extra care needs to be taken as far as personal data is concerned as most jurisdictions impose stringent limitations on the sharing of personal data. The latest example is the California Consumer Privacy Act of 2018 (which will start to apply from January 2020), which imposes significant restrictions on most forms of data sharing by companies. It includes specific rights for data subjects to opt out of the sale of their personal data and the activity of "selling" is defined particularly broadly.

Closing thoughts

From a commercial perspective, there are still many moving pieces and many unanswered questions when it comes to leveraging and protecting data as a business asset. Businesses should continue to explore their data use cases, keep an open mind when it comes to data sharing initiatives but consider the commercial and legal implications of disclosing their data and contemplate contracts as one (though not perfect) option for controlling access to, and use of, their data by others.

> "Data is the new oil. It's valuable, but if unrefined it cannot really be used. It has to be changed into gas, plastic, chemicals, etc. to create a valuable entity that drives profitable activity; so must data be broken down, analyzed for it to have value."
>
> **Adrian Lawrence**

Authors:

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

Adrian Lawrence
Partner
Sydney
adrian.lawrence@bakermckenzie.com

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

Taxing the digital economy: the key role of data

Working out the value of data and monetising data effectively is key to operating a successful business in the digital economy. As much as businesses are working out how to derive value from data, governments are grappling with how to tax the value attached to that data. Diverging approaches are emerging across the world and as any tax imposed on the value created through data ultimately reduces the value of that data for the business, the emerging schools of thought deserve close attention, even at this early stage, to enable businesses to plan effectively.

What has been happening at international level?

Tax regimes around the world have been evolving at an unprecedented speed in the past few years due to the programme initiated by the OECD back in 2013 to counter BEPS – "base erosion and profit shifting". Most recently, the OECD/G20 agreed on a framework for addressing the tax challenges of the digital economy. As businesses have changed the way they operate in the digital environment, the conventional tax rules are regarded by many as no longer adequate to ensure that multinational corporate groups pay their "fair share of tax". The current international focus is on (a) new profit allocation and nexus rules, and (b) a global anti-base erosion/ minimum tax.

The BEPS programme was initiated by the G20 countries to agree a new international tax system, and its reach is extensive. To date, the BEPS programme has received endorsement by over 125 countries (including non-OECD members) under the BEPS Inclusive Framework. At the same time, different countries have been introducing their own unilateral measures to address concerns raised by the OECD as well as to preserve their share of the tax revenue. The reforms driven by the BEPS programme have therefore, to an extent, evolved into political arm-wrestling.

What are individual countries doing?

In **Europe**, the Commission (EC) proposed an interim Digital Services Tax (DST) in March 2018 to address the fiscal concern that multinationals operating in Member States should pay their fair share of tax linked to user activities (and the revenue generated thereby) in those Member States. The EU DST is therefore premised on the principle that in relation to data, value should be attributed to the location of user activities. Furthermore, the tax – usually at around 3% – is imposed on gross revenues (as opposed to profits) from specific digital services such as the provision of digital interfaces or the sale of data for advertising purposes. For example, businesses that operate social networks, search engines or online marketplaces monetise data through user activities. Whilst the EC proposal lacked the necessary consensus agreement to move forward, several EU Member States are in the process of implementing their own version of a DST. **France** enacted its DST at 3% (similar to the EC proposal) on 26 July 2019. Its provisions however take effect retroactively, applying from 1 January 2019. This new law is already being investigated by the **US** under its trade laws, as it is viewed as discriminating against **US** tech companies and unfair in its operation. The **UK** has published its proposal for a DST levied from April 2020 at 2%. Similarly, **Spain** is in the process of finalizing a new law implementing a DST at 3%, while the **Czech Republic** has proposed a 7% tax.

The **US** takes a fundamentally different approach and argues that it is the marketing intangibles and not the user activity that create the value. These include the digital platform, the technology, the R&D as well as the knowledge linked to the development of that platform. Part of the US tax reform under the Tax Cuts and Jobs Act of 2017 included an incentive to encourage businesses to bring their intellectual property held offshore back to the US, so that the value can be taxed in US.

China on the other hand is taking a "wait and see" approach. It has been developing its own transfer pricing regime to ensure that any activities occurring within China will be brought into the PRC tax net. Given China has been embracing globalisation in its economic policy, it also wants to ensure that any tax reform is finely balanced so as to not compromise the wider economic initiatives. Other parts of Asia, such as **Hong Kong** and **Singapore** are also trying their best to accommodate the requests of the OECD without eroding their status as "tax-friendly" countries. This is in contrast to other jurisdictions, such as **India** and **Malaysia**, which have been looking to introduce unilateral measures similar to the EU to protect their tax revenue.

Authors:

Kate Alexander
Partner
London
kate.alexander@bakermckenzie.com

Dominika Korytek
Partner
San Francisco
Dominika.Korytek@bakermckenzie.com

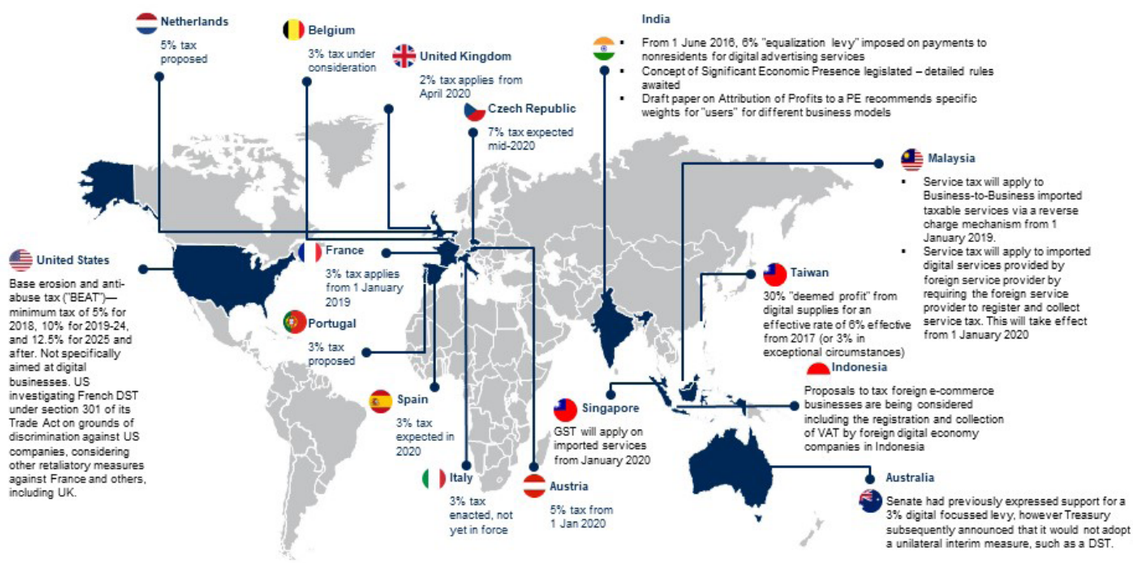
Carrie Lui
Special Counsel
Hong Kong
Carrie.Lui@bakermckenzie.com

How can businesses prepare for change?

The variability in approach among the countries will make it harder to manage tax compliance. It also potentially exposes businesses to double taxation which, of course, would ultimately reduce the value created through data. To prepare for and minimise the impact of changing tax regimes, businesses should work with their advisers to develop a long-term business plan that can weather future tax changes.

Furthermore, notwithstanding that several countries are implementing different unilateral measures, the tax changes around the world do have one common theme. All countries have been introducing rules to increase transparency so that local tax authorities can access information about taxpayers' wider operations beyond their local jurisdiction and in certain cases, exchange it with other tax authorities. Any steps that may trigger a local tax registration obligation should be discussed with advisers to understand how that obligation could affect a business's overall tax strategy.

For a brief summary of the different approaches across the world see our infographic below



CLICK HERE TO VIEW

Data compliance in the data economy - an ongoing balancing act

In the data economy, businesses are facing the tension of leveraging data (personal and non-personal) to stay competitive while keeping in compliance with a myriad of evolving data privacy and security laws and meeting heightening consumer expectations. This is a challenging balancing act. The burden of complying with constantly changing and evolving regulatory requirements is enormous, not least because regulations have an increasingly wide extra-territorial scope and differences between local regimes continue to exist. But there is benefit in taking compliance seriously, in addition to the advantage of reducing the risk of costly fines.

Turning the compliance burden into competitive advantage

The GDPR is still the most prominent example of recent and profound change in data privacy regulation and - due to its wide extra-territorial scope - has increased immensely the regulatory complexity that global organizations now need to navigate. However, on the positive, achieving GDPR compliance brings flow-on effects in terms of commercial opportunities. Largely due to the GDPR, many organizations across continents have now assessed in-depth the personal data they hold. They have then accounted for how they protect and collect, use and disclose that data. To comply with the GDPR, organizations have needed to think critically about the justification for each collection, use and disclosure of personal data, as well as about the time data is kept. The GDPR has resulted in many organizations developing new skills and processes for handling personal data which in turn has given those organizations a better understanding of what data they hold and the boundaries of lawful data processing.

The new knowledge, skills and processes coming with increased personal data compliance can be turned into a competitive advantage. Take the example of a commercial opportunity to utilise data that could be undertaken by one of two businesses. Business A has implemented a comprehensive personal data compliance regime. Business A already knows what data it holds, permitted uses and options such as whether, if needed, data can be de-identified to action the commercial opportunity within the bounds of data protection laws. In contrast, Business B has not reviewed the data it holds or undergone any data protection compliance exercise. Business B would need to do an assessment to work through the issues necessary to determine whether or not it can take advantage of the opportunity (starting with an assessment of whether they have the relevant data and its permitted applications). This may hold up Business B and give the more data-savvy Business A the advantage to be nimble and capitalise first on the commercial opportunity.

And yet, compliance remains burdensome

Turning to the less positive aspect of data privacy and security regulation - the compliance burden. As if complying with GDPR was not hard enough, multinational businesses face the further challenge that even if they are GDPR compliant and they are willing to apply the high GDPR standards across their operations, that may not make them compliant with the data protection laws in non-GDPR jurisdictions.

Rather, significant practical challenges arise for organizations wishing to roll out GDPR-like privacy policies and compliance regimes in non-GDPR jurisdictions. For example, the content required for a GDPR compliant policy (e.g., to inform data subjects about their GDPR rights) might misrepresent the data privacy protections of another jurisdiction which grants fewer rights to data subjects. Additionally, the legal basis to collect and process data may differ from one jurisdiction to another, meaning a one-size-fits-all approach won't work. For example, for direct marketing activities in one country the legitimate interest of the company may suffice, whereas in another country consent of individuals may be necessary. In practice, this will force organizations to still tailor their compliance efforts to individual local requirements or risk non-compliance.

What detail to include in a data privacy notice

Despite a trend for data privacy and security legislation to align globally, there are still many differences between local laws making global compliance a real challenge. For instance, to draft a global data privacy notice is near impossible as the requirements as to what information needs to be included varies widely between countries.

Trends in data privacy regulation

There are jurisdictional differences in the drivers for data privacy and data protection regulation. There are also new data protection laws either just enacted or in development. This is particularly the case in Asia. In many cases, the new laws are enacted in the form of broadly stated requirements dependent on further implementing regulations or other regulator guidance. One of the impacts of these new laws, guidelines and regulations has been business uncertainty over what organizations must do to comply with the new regulatory regimes, in particular what security standards they must meet or what data needs to be kept in-country.

Technology trends such as big data are also impacting data regulation. Many organizations are looking at initiatives to make use of data analytics. These initiatives raise questions about whether personal data is being used, whether it can be de-identified before use and whether ethical or appropriate use of data is being made. Several governments have been developing and issuing frameworks and guidelines for use of personal data for data profiling and monitoring purposes. Organizations are watching for further regulation in this space.

Last but not least, when assessing whether their data practices are legally compliant, organizations increasingly need to consider not just data protection and cybersecurity laws, but also the impact and requirements of competition and consumer laws. There is an increasing interplay among these areas with competition agencies looking closely at the role of data from a competition and consumer law perspective (also see our antitrust chapter). As a result organizations increasingly need to consider their practices in terms of data collection and management from multiple regulatory perspectives.

READ REPORT

Baker McKenzie's Global Data Privacy & Security Handbook

READ REPORT

Baker McKenzie's Short Guide to Data Privacy & Security Regulation and Enforcement

Authors:

Anne Petterd
Partner
Singapore
Anne.Petterd@bakermckenzie.com

Francesca Gaudino
Partner
Milan
Francesca.Gaudino@bakermckenzie.com

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

Michael Egan
Partner
Washington, DC
Michael.Egan@bakermckenzie.com

Jay Zhenyu Ruan
Partner
Shanghai
Zhenyu.Ruan@bakermckenzie.com

Digital antitrust: a global snapshot of latest developments

Digitalisation continues to reshape industries and economies with huge advantages for business and society. But the growth, strength and influence of tech companies remains a mounting concern for many antitrust agencies.

Sometimes under political pressure, many agencies are asking themselves whether existing antitrust rules and procedures remain fit for purpose or need to be supplemented with new rules, concepts, enforcement policies and even regulation. The overarching theme of the International Competition Network's 2019 annual meeting was 'digital'. Over a hundred antitrust agencies from all over the world shared their ideas on what digitalisation means for mergers, cartels and abuse of dominance.

Authors:

Creighton Macy
Partner
Washington, DC
Creighton.Macy@bakermckenzie.com

Samantha Mobley
Partner
London
Samantha.Mobley@bakermckenzie.com

Stephen Crosswell
Partner
Hong Kong
Stephen.Crosswell@bakermckenzie.com

Carolina Pardo
Partner
Bogota
Carolina.Pardo@bakermckenzie.com

Grant Murray
Lead Knowledge Lawyer
London
grant.murray@bakermckenzie.com

Europe

Europe has already witnessed high profile enforcement in relation to the digital economy focussing on, but by no means limited to, abuse of dominance. Investigations have even sought to challenge core business models, arguably pushing the boundaries of antitrust laws. Detailed policy work has resulted in wide-ranging and controversial recommendations that would have major ramifications for the digital economy.

In March 2019, the UK Government published a report by an expert panel led by Harvard economist and former White House economic adviser, Jason Furman, on reforms to competition rules and regulation in the digital sector: "Unlocking digital competition". One of the key recommendations of the UK Furman report was to introduce a digital markets competition regulator with special powers to regulate significant players in digital markets including by developing a code of competitive conduct applicable "only to particularly powerful companies", i.e., those designated as having "strategic market status". The panel's recommendation is consistent with the notion of 'participative antitrust' promoted by Nobel-Prize-winning economist Jean Tirole as a means of addressing competition problems in digital markets. The Chairman of the UK Competition & Markets Authority has also recommended major changes to the competition and consumer law regime in light of the increasing digitalisation of the economy.

In April 2019, the European Commission published a detailed expert report titled "Competition Policy for the Digital Era" on how competition enforcement should evolve to deal with "novel" issues raised by the digital age. The EU Commission is reflecting on the large number of recommendations contained in this report but has already embarked down a regulatory path in the form of a platform-to-business regulation. The regulation was adopted in June this year and will start to apply on 12 July 2020. It aims to address what the Commission perceives as an imbalance of power between large digital platforms and their users. It establishes a legal framework which guarantees transparent terms and conditions for business users of online platforms, as well as effective possibilities for redress when these terms and conditions are not respected. To that effect, the EU regulation includes a range of requirements for online intermediation services to be more transparent about their practices, including by describing any differential treatment they give to themselves.

Perhaps encouraged by these policy recommendations, antitrust officials in the EU are quick to describe the impact of network effects and data sets, the "enduring" market power of certain players and consequent "special responsibility" not to impair the competitive process. More inquiries and investigations seem inevitable.

Asia Pacific

In the Asia Pacific region, governments and antitrust agencies acknowledge the roles of data and digitalisation in driving economic growth. China accounts for 40% of the world's e-commerce and it is estimated that by 2030, the digital sector will enable USD 5.5 trillion of economic activity in China.

And yet an active policy debate is underway in some countries. Australia, Japan and Korea are each reflecting on how to address antitrust concerns in relation to digital markets and the debate is similar to that playing out in the EU. Indeed, the Australian Government is currently considering the Australian Competition and Consumer Commission's recommendations for comprehensive reforms following its inquiry into digital platforms. These include amendments which would enable the Australian antitrust agency to take into account loss of potential competition and the impact of data when assessing mergers.

The Americas

The US antitrust agencies are among those examining the digital economy in some way. For example, in July 2019, the Department of Justice Antitrust Division announced an, at this point undefined, antitrust review into "market leading online platforms", and the Federal Trade Commission has held hearings—as part of its Hearings on Competition and Consumer Protection in the 21st Century—on certain aspects of "technology-based platform businesses" as well as issues involving big data. While, like in many places, these issues are receiving significant scrutiny, and it is expected that this will only continue, the US agencies have also emphasised the need to evaluate claims about data cautiously, and they have stressed the importance of evidence-based enforcement within the existing legal framework and the flexibility of the consumer welfare standard.

In Latin America, antitrust regulators appear to be in the early stages of analysing digital markets. The Mexican antitrust agency published a report in February 2018 analysing the digital economy from a competition law perspective, while the Brazilian authority has launched an investigation into platforms.

Outlook

Overall, the digital economy and the pace of change is clearly adding pressure to many agencies. On the one hand, agencies need to be able to defend themselves against accusations of under-enforcement (and be able to reassure governments about this). But, on the other hand, they must also preserve incentives to innovate and avoid raising regulatory barriers to competition.

The US antitrust agencies, among others, are right to issue, at times, the reminder that agencies should remain disciplined in order to reduce the risks of interfering with fast-moving markets. Enforcement activity should be reserved for situations where there is evidence of actual or likely harm. It is our view that there are good grounds to argue that the existing antitrust toolbox is sufficiently flexible to address antitrust concerns arising in the digital economy.

Open Banking – Challenges and opportunities for new innovative financial services

Authors:

Dr. Manuel Lorenz
Partner
Frankfurt
Manuel.Lorenz@bakermckenzie.com

Adrian Lawrence
Partner
Sydney
adrian.lawrence@bakermckenzie.com

Anne-Marie Allgrove
Partner
Sydney
anne-marie.allgrove@bakermckenzie.com

Karen Man
Partner
Hong Kong
Karen.Man@bakermckenzie.com

In the modern world, it is undeniable that data is a valuable asset, sometimes referred to as the "oil of the 21st Century". 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.

As far as the banking industry is concerned, banks hold an abundance of confidential information about their clients by the very nature of the service they provide. They also collect further data as a part of regulatory requirements. Greater rights for both individual and business customers to access and direct transfers of data held by service providers in the financial services sector 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.

Two key jurisdictions in which legislation is being implemented in this space are the EU, with the Payment Services Directive, and Australia, with the Consumer Data Right. Other jurisdictions, including Hong Kong and Singapore, are also considering similar developments, either on a legislated basis or via an opt-in approach driven by the banks and financial institutions themselves.

PSD 2

A key example of this phenomenon is the recast Payment Services Directive (EU) 2015/2366 (PSD 2) in the European Union, which is not just another restrictive piece of legislation. PSD 2 is also a game changer because it accelerates the already on-going digitalisation of the financial industry by requiring banks to open their payments infrastructure and client data assets to authorised third party service providers. In other words, PSD 2 has paved the path for open banking. Open banking is a banking market where the control of personal data is placed in the hands of the customer. The customer can choose to benefit from third party services by allowing them access to personal data. The banks cannot refuse to provide access to third parties following approval by the customer.

The history of third party access to bank data initially goes back to alternative payment services for online payments (now called PISPs or payment initiation service providers). Merchants integrate a payment solution on their website, under which the PISP opens a "tunnel" into the customers' online banking. The customer uses this tunnel to instruct the bank to wire the purchase price to the online merchant. The PISP then confirms that the payment was instructed and in reliance on this payment, the merchant ships the merchandise to the customer.

Other service providers (AISPs or account information service providers) offer mobile apps that aggregate bank account information for customers using the same type of technology.

In the past, this has raised several issues. Firstly, the third party service provider is involved in the payment chain without touching the money, but is handling very sensitive data, such as the bank customers' login credentials and has access to the customer's account to instruct the payment. Furthermore, by handing these credentials to the third party, the customer is arguably in breach of the obligations towards the bank to not share the login information. Thirdly, the third party uses a customer access and "pretends" to be the customer, which might not be visible to the bank ("screen scraping").

PSD 2 now requires these PISPs to become regulated payment institutions. AISPs merely need to register with the competent authorities without getting licensed. On the other hand, PSD 2 forces banks to allow these third parties to access the bank's systems (with the consent of the customer) via a dedicated interface (API). Banks may switch off other means of third party access if they can show the API is reliable. Both banks and the AISPs/PISPs have cooperation obligations and must ensure data security and confidentiality. AISPs and PISPs must identify themselves when accessing the accounts.

In addition, PSD 2 has significantly beefed up security of online payments by requiring "strong customer authentication" (SCA) – even if merchants, banks and credit card payment processors are currently struggling to implement the new requirements in a timely and customer-friendly manner. Therefore, the European Banking Authority has allowed national regulators to exercise leniency in enforcing SCA. Still, SCA and open banking must be seen together and enter into force on the same date: 14 September 2019.

Consumer Data Right

The Australian consumer data right legislation provides a framework for implementation of the consumer data right which will provide consumers and businesses with a right to efficiently and conveniently access specified data in relation to them held by businesses, and to authorise secure access to this data by trusted and accredited third parties. The consumer data right will also require businesses to provide public access to information on specified products they have on offer.

The consumer data right will apply to specific sectors of the Australian economy which are designated by the relevant Minister (the Treasurer), on recommendation of Australian Competition and Consumer Commission (ACCC). The right will initially apply to the banking sector with the government committing to subsequently extending the consumer data right to the energy and telecommunications sectors, with others to follow.

Potential benefits and services

Both PSD 2 and the Australian consumer data right has the potential to open up a level playing field for all service providers including third party service providers.

The possible fields of application have not yet been fully explored, but the following business models have emerged so far:

- Aggregation apps for money management/personal finance. The provider uses the data to make suggestions to the customer regarding financial products and services and earns a commission on product sales.
- Alternative payment method for online dealers.
- Instant credit approval solely based on access to the borrower's payment data.
- Identity check.
- Advice on savings and investments based on an analysis of a customer's current investments.
- Other value add services.
- Banks integrating the customer's accounts held with other banks into a single online banking solution.
- Service provider to unregulated FinTech companies which need access to bank account data.

Despite the cost of increased security measures, the reward for entering the FinTech markets can be very significant, owing to customer expectations. As these developments remove barriers for non-banking entities, this has opened up the market for new entrants with fresh ideas. Clearly, there is more competition in the banking industry as banks are no longer competing just amongst themselves, but with FinTechs too. However, this allows banks to pursue an ecosystem by including third party services as their primary services thus extending scope for innovative business models and increased revenues. This will also result in an overall infrastructural advancement as the procedures will be more cost and time efficient.

The future of work in the data economy

The digital age is fundamentally changing the way we work. With traditional contracts of employment and offices on the decline, contingent and remote workers increasingly the norm, and digital well-being becoming the subject of legislation, organizations must adapt and evolve. reorganize their workforce. This includes, for example, finding the right balance between taking advantage of HR analytics while not engaging in inappropriate employee surveillance, allowing the workforce to work flexibly, but promoting healthy digital behavior, and automating processes and tasks while adding new skillsets to the human workforce.

The right to digitally disconnect

The rise of technology has blurred the line between work and private life. Widespread use of digital devices has resulted in increased remote access creating a culture that assumes instant availability. While some employees appreciate the increased flexibility that comes with remote working, it comes at a price. Legal issues arise over excessive working time as well as health and safety with techno stress, tele pressure and digital fatigue as a direct result of ever-present connectivity.

In response to growing concerns, some employers have taken it upon themselves to put practices in place to allow employees to disconnect and adopt sustainable digital behavior. Examples include sending emails back to the sender when the receiving employee has logged off, auto-deleting emails sent to someone on leave, or banning the sending of emails outside of working hours. In a survey of global companies conducted in partnership with Wired Magazine, we found that 74% of participants felt companies needed rules to avoid an "always-on" work culture.

In addition, legislators including in France, Italy, Belgium, Germany, Spain, Luxembourg, the US, Colombia and the Philippines, are starting to regulate digital disconnection. France took the lead in 2017, enacting a law requiring companies with more than 50 workers to draw up a charter of good conduct, setting out the hours when staff are not supposed to send or answer emails, while Spain and Italy have since adopted similar laws, requiring companies to implement measures to clarify the right to disconnect outside of working hours. Legislators are also responding to the need to protect the limits on working hours with increased compliance obligations, such as the requirement to accurately and reliably record employees' daily working time, which the European Court of Justice ruled on earlier this year and which applies to all EU member states.

> "Companies can help employees disconnect – not just because it's the right thing to do, but also to increase their productivity during working hours.".
>
> **Meredith Kaufman**

As vast differences exist in attitudes to working hours, physical presence of workers, industry demands and the composition and location of teams, the concept of disconnecting cannot be seamlessly adopted across borders or industries. However, there is a clear trend towards regulating the right to disconnect, and employers that leverage the benefits of a flexible, always connected workforce, would be prudent to monitor the direction of travel not only to anticipate and prepare for new regulatory requirements, but also to ensure they are looking after and protecting their workforce. As digitalization grows, expect the conversation around employees' digital well-being to continue.

The ethics of HR analytics

Many employers are grappling with both the opportunities and challenges of employee data analytics. On the one hand, the use of analytics and AI in workforce management can generate vast improvements and provide a competitive advantage. On the flipside, there is a real risk of inappropriate employee surveillance and loss of trust.

For instance, the use of wearables, such as smart phones and watches, to collate rich sensor data allowing employers to track stress and efficiency levels can help identify when an employee is at maximum efficiency and when to reallocate tasks. It could also help promote awareness amongst employees of their work habits, highlight a need to disconnect and empower them to recognize and address personal habits to achieve a more balanced and productive work life. Similarly, employee data can be used to analyze and optimize factors such as employee engagement, performance, productivity, equality of pay and benefits, health and more. But where do employers draw the line to ensure they don't engage in inappropriate monitoring or tracking and lose employee trust?

> "Unions are now articulating their concern about employers using employee data for purposes beyond those for which the data was originally collected."
>
> **Fermin Guardiola**

Another challenge is avoiding bias. The use of talent analytics and employee screening with AI allows for the automation of many mundane and time-consuming operations – scanning CVs, conducting interviews and even analyzing employee mannerisms. In the best cases, this can improve the diversity of candidates; but algorithms may unwittingly perpetuate existing bias, having the opposite effect of what is desired.

> "Any algorithm is only as good as the data that has gone into it. You need to be able to evaluate what's happening and keep a close eye on it, to check for potential bias or disparate impact."
>
> **Meredith Kaufman**

The opportunities that AI presents in the workplace are significant, but these need to be monitored and balanced carefully against our ethical and social values. Using technology to invest in employee talent, skills and culture can bring about huge benefits for organizations, but the challenge is in using it the right way.

The rise of automation and the impact on the workforce

With machine learning making it increasingly possible for machines to perform high-level cognitive tasks, there has been a marked concern about increasing unemployment. One study showed that whilst 47% of jobs could be at risk of being replaced by automation in the US, this was as much as 72% in China and 77% in Thailand. In South Korea, a tax on robots is already in place, to make up for the loss of tax revenue from unemployment. However, research focusing on the impact of automation on job tasks rather than whole occupations tells a different story. McKinsey estimates that while 51% of work activities in the US could be automated using current technology, fewer than 5% of occupations could be entirely automated, and the OECD found that only 9% of jobs on average are at risk across the 21 OECD countries.

There are reasons to be optimistic, and the fear that robots will replace human workers at large may not be justified. There has been a strong pattern through time for repetitive and routine tasks to be increasingly performed by machines, but at the same time many new jobs have in fact emerged, requiring human skills such as manual dexterity, higher cognitive skills, management and social interaction.

While the impact of automation will vary between countries and industries, there is no doubt it will transform the world of work, and companies will need to find the balance between automating tasks and processes while retraining and re-organizing their human workforce to collaborate with technology.

Authors:

Fermin Guardiola
Partner
Madrid
Fermin.Guardiola@
bakermckenzie.com

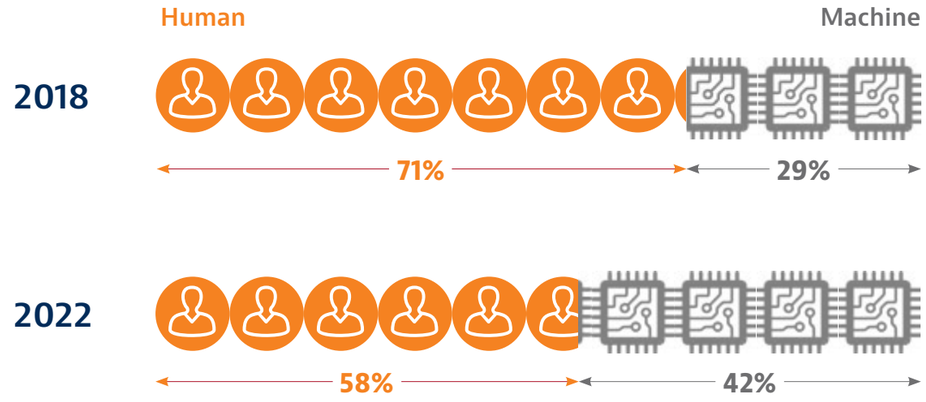
Meredith Kaufman
Partner
New York
Meredith.Kaufman@
bakermckenzie.com

Rowan McKenzie
Partner
Hong Kong
Rowan.McKenzie@
bakermckenzie.com

Penny Darragh
Knowledge Lawyer
Belfast
Penny.Darragh@
bakermckenzie.com

Rate of automation

Division labor as a share of hours spent (%)



*Future of Jobs Report 2018, World Economic Forum

Blockchain – New technologies benefiting from and enabling the data economy

Authors:

Sue McLean
Partner
London
Sue.McLean@bakermckenzie.com

Gavin Raftery
Partner
Tokyo
Gavin.Raftery@bakermckenzie.com

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

Blockchain, which has been hailed by commentators as the next generation of the Internet – the "Internet of Value", (Don Tapscott & Alex Tapscott, Blockchain Revolution) is far more than just the technology behind Bitcoin. However, the key question hanging over this technology remains – will a breakthrough use case emerge outside of cryptocurrencies?

Blockchain, or more generally distributed ledger technology, is a general-purpose database technology for creating secure, peer-to-peer applications that creates a decentralised and tamper-evident record of transactions and other data, synchronised across the computers of participants (nodes) of the network.

Developments in use cases

While financial services use cases remain the most developed, Baker McKenzie has seen an increased interest in blockchain from clients across a range of industries. Use cases include supply chain tracking and verification, decentralised apps, healthcare, energy management and identity (including academic and professional credentials).

However, existing projects are almost all at a proof of concept stage and this relative immaturity is a challenge. Gartner, Inc. predicts 90% of current enterprise blockchain implementations will require replacement by 2021 in order to remain competitive, secure and avoid obsolescence.

Compounding this issue is that many potential users are still uncertain about the benefits blockchain adds to their existing processes and technologies – the old adage of "a solution without a problem".

Regulatory approaches

In 2017 and 2018, initial coin offerings (ICOs) or "token sales" grabbed the headlines. These were an alternative model for start-ups to raise finance quickly, in many cases without jumping through the regulatory hoops applicable to IPOs. Regulators around the world have taken divergent approaches to ICOs, some banning them outright, and others considering them under existing securities laws on a case-by-case basis. Aside from certain regulatory pronouncements and guidance specifically focused on crypto-assets, many regulators have taken a "technology-neutral" approach to blockchain, holding that blockchain should be viewed through the lens of existing sector-and-issue-specific regulations and that new laws are not required at this time.

However, some commentators have questioned whether the fundamental nature of blockchain technologies will allow them to comply with certain existing laws. In particular, many have suggested that blockchain is incompatible with the EU's GDPR, designed as it was for a centralised world of data controllers and data processors, in particular its data minimisation obligations and rights of erasure which conflict with the perceived immutable nature of the technology.

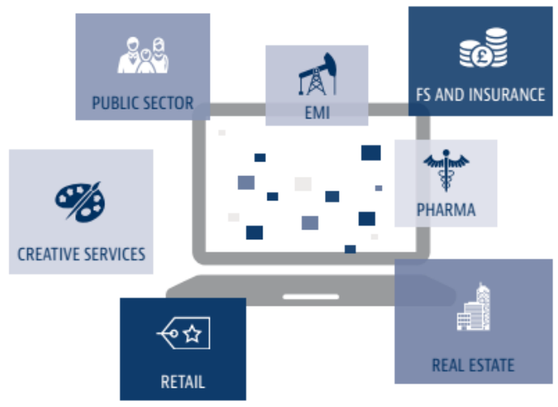
To date, we only have published guidance on data issues raised by blockchain from the French regulator, CNIL. In its report, CNIL has acknowledged the potential incompatibility and presented useful suggestions on how to tackle GDPR compliance when approaching blockchain projects (see our client alert here), including that participants should use permissioned blockchains wherever possible (i.e., those that are open only to specific, invited participants and closed to everyone else) and that personal data should be held off-chain. However, the regulator stated that clarity on certain issues was required and has looked to the European Data Protection Board (EDPB) to provide guidance. Unfortunately, it's clear from the EDPB's roadmap that blockchain is not currently high on its list of priorities.

Accordingly, for now, parties should apply existing law to their blockchain projects, but keep an eye out for relevant legal and regulatory developments.

READ REPORT

Baker McKenzie's Unhashing Blockchain report

Applications across Industries



Contracting for blockchain

In addition to corporate JVs and traditional service-provider-customer models (e.g., licensing terms), multi-party and consortium agreements are another common approach for blockchain projects. These consortiums, often between traditional competitors and other industry stakeholders reflect the collaborative approach that is needed in order for blockchain to be truly transformative in respect of a particular sector as a whole.

The need to manage relationships among consortium members has influenced their structure. Very few enterprise clients will consider participating in open ("unpermissioned") networks because of the compliance challenge. While proof-of-concept agreements are relatively easy to put together, the issues in a full participation agreement are more complex. The parties will need to address the relevant risks raised when live transactions and data are being processed by the platform, including how liability is apportioned between members, how disputes will be governed and who will own which parts of the infrastructure and software on which the blockchain is built, particularly where various members have contributed to the platform's development.

Looking Ahead

It's still early days in the development of this new technology and while many current blockchain projects may fail, this exploration phase is important in helping identify credible use cases. As some of the hype recedes, we are starting to see a more measured approach to the use of blockchain, rather than seeing it as a magic pill for all scenarios.

There is now a general acknowledgment that the most ambitious projects will take significant time and effort and will require the patience, stamina and ongoing commitment from participants to fulfil their true transformation potential. This realism is a positive sign if blockchain is to become an established technology underpinning the new data economy.

New Infrastructures – Automated and connected vehicles, smart roads and smart infrastructure

Authors:

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

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

Rico Chan
Partner
Hong Kong
Rico.Chan@bakermckenzie.com

Autonomous mobility is a prominent feature of an increasingly interconnected world where the Internet of Things impacts not only vehicles, trains, aircraft, drones or other movable assets, but it also plays a significant role in our cities, our buildings, roads, and supporting infrastructure like airports and ports. It reflects on the way we work and live, with a massive amount of data and information flowing among machines and requiring all players and stakeholders to be cognizant of its potential.

The pace of 'smart' industry

According to high-profile analysts, volume commercial deployment of fully Automated Vehicles (AVs) worldwide is predicted to be 10 years away. However, key industry players aim to have vehicles equipped with Level 4 Automated Driving Systems, which allow vehicles to perform all driving functions in as soon as 2 years in certain markets. Several manufacturers are already testing this technology worldwide, with both real on-road trials and simulation miles run in the cloud.

EU Member States are boosting support for AV industry and related testing. Notable examples, among others, are:

- the United Kingdom where, in March 2019, the Centre for Connected and Autonomous Vehicles published the Future of Mobility: Urban Strategy paper, setting out the governmental approach on automated and connected mobility innovation and related regulatory review; and
- Italy, where the Roads Monitoring Center issued, in Spring 2019, its unanimous official affirmative opinion on the first application to test AVs on public roads.

In the United States, the Department of Transportation published its latest policy update in the fall of 2018. Preparing for the Future of Transportation: Automated Vehicles 3.0 (AV 3.0) provides further guidance on DOT's existing policies, including the use of voluntary safety standards and the proper roles for the Federal and State governments, and also expands DOT's guidance beyond passenger vehicles to other modes of transportation.

AV 3.0 sets forth DOT's six "automation principles" — (1) prioritizing safety; (2) remaining technology neutral; (3) modernizing regulations; (4) encouraging a consistent regulatory and operational environment; (5) preparing proactively for automation; and (6) protecting and enhancing the freedoms enjoyed by Americans. These principles are reflected throughout AV 3.0 and DOT intends to translate these principles into action through stakeholder engagement, best practices, voluntary standards, targeted research, and regulatory modernization.

- More than 80 companies across the U.S. are already testing self-driving cars, trucks and other vehicles – an estimated 1400 vehicles are currently in testing.
- Over 1.59M drones are currently registered in the U.S. – nearly five times the number of registered manned aircraft.

The technical knowledge and scientific know-how related to the integration of automation technologies into vehicles is already accessible. However, AVs' actual deployment has to endure other technical challenges, such as the complex interplay among the broad range of Machine to Machine communications which include V2V (Vehicle to Vehicle), V2I (Vehicle to Infrastructure), V2G (Vehicle to Grid) and V2X (Vehicle to Everything) interconnections. These technologies require a highly reliable and low latent connectivity in order to be able to convey communications continuously and seamlessly. The choice of a common connectivity standard, such as 5G or WiFi, is therefore a core decision for the flourishing of these new infrastructures.

Main regulatory trends

The starting point for this development was the adoption of EU Reg 2015/758, by means of which the European legislator introduced the interoperable EU-wide eCall, a mandatory requirement applying to all new vehicles from 31 March 2018. Thanks to this IoT mandatory tool, in the event of a severe accident, vehicles must be able to automatically contact the EU emergency number (112) and transmit location and other data to emergency services. For its part, the United States currently favors an industry-driven, technology neutral approach, and some U.S. manufacturers offer similar services on their vehicles.

Following this initial regulatory milestone, the implementation of IoT in movable and non-movable assets has evolved towards enhancing human driving capabilities, improving road safety and achieving a higher social inclusion. However, for cities to be smart and connected with other machines, it is necessary to develop a legal framework that sets out the boundaries for their lawful operation.

Addressing new challenges: ethics and liability

As the application of IoT technologies in this field often entails machines engaging in decision-making activities, regulators have to take into account ethics-related aspects (e.g., by mapping ethical frameworks to guide AVs' algorithmic/software design decisions). Although there are only few examples (see the German Report on Automated and Connected Driving), the debate has been the subject of many experiments. The Massachusetts Institute of Technology developed the so-called Moral Machine, a global survey in the form of an online game that gathered human judgements on acceptability of ethical decisions made by automated driving systems in various accident scenarios – needless to say, the outcomes were far from conforming.

Alongside the challenging debate around ethics and algorithms, one of the other aspects curbing the widespread dissemination of these new infrastructures relates to the liability regime surrounding AV's circulation. Most jurisdictions are currently consulting to identify appropriate solutions to regulate various aspects such as:

- the applicability of civil negligence and what exclusions may be granted, e.g., duty of care, breach of duty and accountability for the resulting damages;
- the criminal liability regime, e.g., corporate manslaughter for defective AVs, liability for compliance with motor vehicle code;
- insurance coverage requirements and liability for OEM and drivers, e.g. whether the OEM will be required to carry insurance;
- the contractual liability between OEMs and the supply chain, e.g. contract caps, indemnities for faulty software.

Conclusions

As the trends are converging to a common and standardized environment, the deployment of next-gen, interconnected infrastructures and vehicles will be shaped by forward-looking guidance. The combination between top-down regulation and industry-led collaboration with regulators is key to the achievement of an optimal balance. AVs and smart cities will characterize the future look of our urban surroundings. New rules will be needed in order to efficiently integrate the existing environment with these new infrastructures.

Disputes in the new data economy

The evolution of the data economy presents new and heightened litigation risks, especially for those at the heart of the ecosystems which drive it.

Authors:

David Halliday
Partner
London
David.Halliday@bakermckenzie.com

Benjamin Roe
Lead Knowledge Lawyer
London
Benjamin.Roe@bakermckenzie.com

Regulators with a renewed focus and powers

The rise of personal data regulation, in particular, has resulted in the development of freshly empowered regulators, with the tools at their disposal to cause a real impact. No one needs to mention the potential size of GDPR fines anymore – and, although there remains some doubt over the appetite of regulators to impose truly significant fines, some – such as the UK's ICO – have recently laid down some meaningful statements of intent in their proposed fines for data breaches.

There is every likelihood of challenges to fines of this size, with public law and procedural fairness questions often at the forefront. With greater power, comes greater responsibility and scrutiny for the regulators involved.

Think broader than privacy

It's not just the personal data regulators who are likely to be involved in the action. There is a broader consideration of how individuals are affected by the use of their data, beyond data protection law. Competition law and consumer law regulators are looking at broader questions of data as a source of market power, and its use as a source of potential unfairness to the consumer. Expect a coming together of the regulatory approaches with respect to significant platform providers in particular.

There are also some growing areas of interest where recent and planned regulation may give rise to more regulatory scrutiny:

- One is the growth of regulation focused on assuring continuity for key assets and services, including those key to the functioning of the digital economy (such as the EU NIS Directive): these have the potential to hit directly or indirectly a number of technology companies, especially those involved in M2M for infrastructure, fintech or healthtech. Though the jury might still be out on how important these regulations turn out to be, they represent another potential risk avenue for a broader number of tech players.
- A second is a "space in between" which legislators are looking to address – security at a device level. With more and more connected devices both sending and receiving greater volumes of data, security on devices themselves looks increasingly key, but the responsibility of device manufacturers and retailers may often fall outside the direct reach of data protection laws. We expect a renewed focus on the use of existing product regulation, product liability and consumer protection laws – and potential revision - to address unsecure devices placed on the market. Device manufacturers/retailers will have to actively ask themselves the question whether the discovery of critical security vulnerabilities is a basis for a product recall, or at least whether they have any active duty to push out patches.

Access to justice (and the funding to get it)

Alongside the rise of substantive regulation which gives greater rights of compensation to individuals, as is typically the case with data protection and consumer protection laws, the mechanisms for how to use those rights are being continually assessed. We continue to see a rise in both collective action mechanisms outside the US, and the actual use of those mechanisms. In the EU, in particular, there has been long running consideration of a new Representative Actions Directive to allow for representative bodies to bring actions on behalf of the consumers whose interests they represent. Although politically difficult and now coming under fresh consideration by a new EU Parliament, a version of the Directive may well be enacted.

In any event, the litigation economy clearly sees the potential in the data controversy market. Litigation funders and claimant law firms are interested, and invested, in the development of litigation against holders of data who have misused it or failed to keep it safe. The substantive regulation to launch consumer compensation claims is in place, and more regular regulatory enforcement action is a clear springboard for it.

Keeping out the bad guys is key

There was a time when it was thought that an organisation might be cut slack around the difficulties of stopping criminal access to data - no longer. Regulators and courts have shown their willingness to come down hard on those who do not take their data safeguarding responsibilities seriously. The rationale seems to be that if you expect to make money off it, expect to look after it, even if the technology, ecosystem complexity and threat actor sophistication make this increasingly difficult. Yet there will continue to be interesting challenges in making claims stick against those who fail to safeguard, particularly around causation: in a world where hacks successfully happen every day, how do claimants successfully demonstrate that any individual data breach event was responsible for the harm they suffered? What if they themselves contributed to the issue with their own poor cyber hygiene, such as password reuse?

We also expect to see more complex litigation in this area, with supply chain actors and ecosystem partners joined as defendants and seeking reallocation between themselves, security providers directly in the firing line, and insurance coverage in particular being tested on a more regular basis. We may also see revisited the sometimes difficult and unclear legal question (in many jurisdictions) of whether regulatory fines can be passed between contracting parties as damages or under indemnities.

Value and ownership

Data is typically difficult to assert IP protection against, and more reliant on the fairly general principles of trade secret law where they exist. The best realistic protection is simply to ensure that no unauthorised third party ever gets access to it – and that trusted parties only do with it what they are explicitly permitted to, before returning it. Talent also presents a unique challenge, with an increasing focus on how to ensure leavers do not abscond with valuable company data assets or other intangibles. With increasingly valuable concentrations of data, metadata, and analytics or machine learning derived data, there is going to be more pressure on putting trade secret laws to the test – in many cases, such as the US DTSA and the EU Trade Secrets Directive, these are relatively recently enacted and untested. It remains to be seen whether they are truly fit for the purpose of protecting data as an IP asset.

Data at the global crossroads

As any asset becomes more valuable, so does its significance in the realm of geo-politics. Just as trade in physical goods is a key part of current geo-political machinations, so is movement of data and access to data. This manifests itself in various ways: in the evolution of various data localisation laws aimed at keeping valuable local data onshore and of limited use to the economy of other countries. These laws create a clear risk for any company doing business in those countries, and the potential to fall foul of local regulatory agencies with an axe to grind against a foreign power. Other trade laws (export control, sanctions) primarily aimed at traditional goods and services are often cast broadly enough to cover data in and of itself, and need to be taken into account. These are not new regulatory issues for global technology companies, but the prevalence of data as the asset itself presents a new challenge.

Lastly, law enforcement and security agency access has not gone away as an issue. Technology companies holding large data sets are going to feel the increased heat of law enforcement access requests, and the continued tension between their duties to individuals, and their obligations to cooperate. Clearly, these challenges often play themselves out away from the public eye, but they are no less complex for that, and present a different challenge in litigation through the development of good government relations as a means of resolution.

Trends in Tech M&A Deals

Authors:

Tracy Wut
Partner
Hong Kong
Tracy.Wut@bakermckenzie.com

Darcy Down
Partner
Chicago
Darcy.Down@bakermckenzie.com

Robert Wright
Partner
Hong Kong
Robert.Wright@bakermckenzie.com

Kirsty Wilson
Partner
London
Kirsty.Wilson@bakermckenzie.com

Drivers in M&A deals

2018 was a record year for tech M&A deals. Technology acquisitions continue to be a driving force for M&A in 2019 (see our 2019 Global Transaction Forecast for TMT here). A few trends have driven deal activities:

- Software and IT developers continue to provide firepower and drive deal value
- VC type deals from both financial sponsors and corporates continue to fund early stage growth of tech companies
- The integration between telcos and content providers continues to develop at pace
- M&A remains the primary focus for exit in the tech sector for founders
- More venture capital investments, partnerships and joint ventures than buy-out acquisitions
- Shift in focus on supply chain, particularly for tech manufacturers in light of trade war related head winds

Due Diligence Focus – Shift

Data. In the past, due diligence on tech targets often focussed on the target's intellectual property as a key source of perceived value. In recent years, we have observed a shift in focus to data, in particular ownership, control and management of data and its use in new tech, automation, machine learning, AI, big-data analytics and more.

The important question is now – how does a company measure or place a value on their data? Recent big data related acquisitions have resulted in mixed views from analysts on the right formula to determine the value in that data. This has led to broad discussion as to whether accounting regulations may change to require listing data as a tangible asset on the balance sheet (or related changes to the classification of this intangible asset). Assignability of data is also a key driver for lot of buyers because it directly impacts revenues.

Importantly, there has been an increase in focus around data privacy enforcement issues as the reputational risk and costs of managing breaches and responding to complaints could be significant. This trend is set to intensify, given – for example – a recent GDPR enforcement action by the UK ICO in a transactional context holding the buyer responsible for the target's insufficient data security practices on the basis that the buyer failed to undertake sufficient due diligence into the target's data security practices during the acquisition.

Offshoring. For IT services, offshoring is increasingly of interest. Aside from satisfying regulatory compliance requirements, there are also commercial implications when offshoring, particularly IT services businesses interacting with regulated financial institutions and healthcare provider customers.

People. Lastly, people remain a key focus. Developers and other key people within tech businesses typically have proprietary information on critical data. A buyer will generally be seeking protection to ensure continuity of service of such individuals post-closing.

Deal Documentation

We are seeing more auctions and fewer bilateral deals. Private equity and traditionally non-tech companies are increasingly active in the technology and data space. The result is seller friendly agreements, with buyers taking back points where they can. We highlight a few key developments below.

Purchase Price. Everyone (including private equity, tech and non-tech companies) is looking to keep up with the pace of innovation. If bidders see a product they like, they will pay a premium for the chance to get or stay ahead of the curve. Fewer buyers are walking away based on price alone. There are very interesting auction dynamics when it comes to valuing data and its impact on the overall purchase price. In the same auction process, the value one bidder places on that data may vary significantly from another and will depend in large part on who that bidder is and how they plan to use the data.

Available Damages. While buyers are paying more in terms of purchase price, they are insisting that they be able to recover the full scope of damages for any post-closing indemnification claims. This includes consequential or indirect damages, diminution in value and damages based on a multiple. Buyers are paying more up front, but want the benefit of their bargain in the event there are material issues discovered post-closing.

Earnouts. Sellers are increasingly seeking to avoid earnouts altogether and instead receive their cash up front at closing. Where we do see earnouts, sellers have been more successful in negotiating post-closing covenants governing a buyer's operation of the business, preventing a buyer from operating the business in a manner that could cause the business to miss milestones, either intentionally or unintentionally.

IP Representations and Warranties. In recent years, new regulation means new focus on data privacy and cybersecurity representation. Due to prevalence of representation and warranty insurance in North America, Europe and increasingly in Asia, we see less focus on higher indemnification caps or longer survival periods. Instead, buyers are tending to push sellers to agree to a broader scope of reps, with fewer (if any) qualifications (e.g., no knowledge qualifiers on the non-infringement rep).

Impact of #metoo. In the last 18 months, we are starting to see specific representations in purchase agreements addressing matters of misconduct or discrimination. These representations frequently have look back periods and no qualifiers. We are also seeing covenants between signing and closing requiring the target to notify the buyer if any allegations are made prior to closing. Most importantly, however, buyers are now tailoring management agreements and equity awards to ensure that individuals who are terminated as a result of misconduct or discrimination would not benefit from that termination.

Post-Deal Integration – the Cultural Issue

Each integration and each deal will have different characteristics. The people are key to any tech business. For post deal integration, the culture piece is one that investors should always keep front of mind. Even when pure tech are buying pure tech, there can be cultural issues. And with more traditional non-tech companies acquiring tech companies, it can bring about additional cultural challenges, which can affect how the businesses are run and the success of any integration.

Technology, Media & Telecommunications Industry Group

Key Contacts

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

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

Jay Zhenyu Ruan
Partner
Shanghai
Zhenyu.Ruan@bakermckenzie.com

Kate Alexander
Partner
London
kate.alexander@bakermckenzie.com

Adrian Lawrence
Partner
Sydney
adrian.lawrence@bakermckenzie.com

Carolina Pardo
Partner
Bogotá
carolina.pardo@bakermckenzie.com

Editors

Anna von Dietze
Lead 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 70 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