TMT

The Australian Landscape

September 2020

CORRS
CHAMBERS
WESTGARTH

corrs.com.au

Welcome to the third edition of *TMT: The Australian Landscape.*

Since our last edition was distributed in late 2019, businesses and communities across the world have experienced tumultuous disruption as a result of the COVID-19 pandemic. But as we start learning how to live and work with the virus, new and changed opportunities have arisen for the TMT sector in Australia.

In light of the significant geo-political and national security issues presently at play, we begin this edition by considering the new changes to foreign investment review in Australia. M&A activity in the technology sector has remained relatively strong during the pandemic, and the proposed regulatory changes will require careful consideration and planning to ensure deals are not unduly disrupted.

The rapid adoption of digital health technologies during COVID-19 may have provided the push the sector needed to find better traction in the Australian market. We discuss the opportunities for significant ongoing growth of the sector if regulatory issues are well managed.

We also consider the review of Australia's controversial TOLA Act, which gave new powers to law enforcement and intelligence agencies to obtain information and assistance from communications providers, look at how learnings from the pandemic are shaping a new approach to outsourcing and outline some of the challenges and opportunities 'big data' and open banking present in the financial services sector.

We also give thought to the rollout of the 5G network in Australia, and consider the ways in which new technologies are being implemented in commercial and residential buildings (including to try to manage health risks) and the effective use of Master Systems Integrators in the procurement model.

Finally, continuing our consideration of the widespread application of artificial intelligence in business, we consider the role of the human author in content created by AI technologies and its impact on copyright subsistence. Unless changes are made to Australia's copyright law, this could have an adverse impact on investment in AI-created content.

Please enjoy this edition and feel free to contact any member of the Corrs TMT team if you wish to discuss.

James North
Head of Technology,
Media and Telecommunications

Frances Wheelahan
Partner

Contents

Draft FIRB legislation: what are the implications for Australian technology transactions?

By Justin Fox, Partner, James North, Head of Technology, Media and Telecommunications and James Wallace, Senior Associate

The Federal Treasurer has released an exposure draft of the legislation that will implement his previously announced reforms to Australia's foreign investment framework.

Among other changes, the legislation will introduce a zero dollar screening threshold on foreign investments into any 'national security business'. This will mean that any direct investment by a foreigner into a national security business will require FIRB approval.

In our June 2020 article, we suggested that this new national security test is likely to have broad application to transactions in the communications, technology and data sectors. The draft legislation has provided further line of sight on the likely implications of the changes for technology transactions undertaken by foreign parties in Australia.

What technology assets will be subject to the new national security test?

The exposure draft provides further clarity on the types of communications, technology and data assets that will constitute a 'national security business' and will therefore be subject to the zero dollar screening threshold. They are:

- Telecommunication carriers and carriage service providers regulated under the Telecommunications Act 1997.

  This includes VOIP service providers, virtual network operators and internet service providers. There had been some concern following the Treasurer's initial announcement that the definition would extend to other business regulated under the Telecommunications Act 1997, such as social media companies and video streaming services. The exposure draft has confirmed this will not be the case.

- Businesses that develop, manufacture or supply critical technologies with a military use or which are intended for a military use.

  The definition captures any critical technology that is used by the Australian defence force or intelligence community, by any of their respective contractors or suppliers or by a foreign defence force in a way that may affect Australia's national security. This will capture emerging military technologies, irrespective of whether the technology has been deployed or commercialised.

  Businesses that supply critical technologies used by the defence force or the intelligence community will be subject to a zero dollar threshold, even where the technology does not have an express military purpose, or the military use is not the main application of the technology. The draft explanatory memorandum notes that many such technologies will not be considered to be 'critical' and will sit outside the test on that basis. However, is not clear how a foreign buyer is to make that determination, as the exposure draft gives no guidance on when particular technologies are to be considered 'critical'. The explanatory memorandum suggests that buyers look to publicly available Defence documents, such as the Defence Industry Policy Statement, Defence Industrial Capability Plan, and the Defence and Strategic Goods List for guidance to form a view on whether the target technology is 'critical'. Some further guidance on that point would assist the final legislation.

- Businesses that store or have access to information that has a security classification.

This will capture data centre providers and hosted platform services working for Australia defence forces and intelligence agencies.

- Businesses that store or maintain personal information of defence force personnel collected by the Australian defence force or intelligence community which, if disclosed, could compromise Australia's national security and businesses that collect such information as part of an arrangement with defence or an intelligence agency.

  Significantly, this category only captures data sets that are collected by or on behalf of defence or intelligence agencies. This means that commercial data sets that include personal information of defence force personnel (such as shopper loyalty schemes) will not be caught.

- Businesses overseen by the Critical Infrastructure Centre (CIC), which at present, includes owners and operators of electricity or gas supply, ports and water infrastructure.

  The list of assets overseen by the CIC is dynamic and can change over time. As discussed in our 2019 article, there is speculation that the purview of the CIC may be extended to cover nationally significant data assets.

Foreign buyers of technology assets will need to determine at an early stage whether the target is a 'national security business'. If so, foreign buyers should endeavour to define the national security concerns presented by the proposed transaction and consider how they might be addressed in the FIRB filing or mitigated by way of undertakings. In this regard, buyers should be mindful of FIRB's growing preference to deal with data security issues by way of access undertakings (see our earlier article here).

Unfortunately, based on the definition on the exposure draft, it will be difficult for a foreign buyer to confidently assess whether or not the target is a 'national security business' without the seller's help, as it assumes a relatively detailed level of knowledge about the target's client base and the use of its technologies.

New call-in powers for the Treasurer

The exposure draft gives the Treasurer new powers to call-in for review any investment which is not otherwise notifiable or already subject to FIRB oversight on national security grounds. Where an action is called in, it will be subject to FIRB review in much the same way as if it had been required to be notified to FIRB in the first place. Transactions can be called in any time, including after completion. In these circumstances, the Treasurer will have the power to either require a divestment of the interest by a foreign person or terminate the relevant agreement.

The call-in powers apply to 'reviewable national security actions'. Interestingly, this concept goes well beyond acquisitions and investments that would traditionally have been subject to FIRB review. For example, it captures any significant agreement which gives a foreign person the right to use the assets of an Australian business. This could conceivably capture a licensing deal for a technology product or data sharing arrangement.

This extension of the Treasurer's review powers brings Australia closer to the position in the US where the Committee on Foreign Investment in the United States (**CFIUS**) has the power to review broad categories of transactions which give a foreign party access to non-public technologies. It will be important for FIRB and the Treasurer to provide guidance to the market on the circumstances in which the call-in power will be used. Without that guidance, foreign parties may feel the need to voluntarily notify FIRB of relatively benign actions, which could clog the approval process.

Last resort powers

The exposure draft also gives the Treasurer the right to reassess and impose conditions on or to unwind previously approved foreign investments. Known as the 'last resort powers', this right will apply where there is a change in circumstances after the initial assessment which gives rise to new national security risks. This includes a material change in the activities of a business or where the circumstances of the market become materially different. This is particularly relevant to technology companies which tend to be focused on the development of new products and are more likely to experience rapid growth in their customer base.

The last resort powers will only be available for actions that were notified to the Treasurer on or after 1 January 2021.

Next steps

Public submissions on the draft legislation closed on 31 August 2020 and the Government intends for the new regime to commence from the start of 2021.

In the meantime, foreign investors will need to comply with the temporary COVID-19 measures and should remain mindful of the changing regulatory landscape when planning foreign investments in Australian communication, data and technology businesses.

Challenges and opportunities facing Australia's digital health sector

By Frances Wheelahan, Partner, James Cameron, Special Counsel, Suman Reddy, Senior Associate and Emily McClelland, Law Graduate

While the COVID-19 pandemic has presented a number of challenges for Australia's digital health sector, it has also accelerated the use of digital health technologies, opening-up potentially significant growth opportunities for the sector.

ANDHealth's recent report on Australia's nascent digital health sector, Digital Health – The sleeping giant of Australia health technology industry, highlights a number of challenges and opportunities facing the sector following the impact of COVID-19.

- The global digital health market is predicted to reach US $505.4 billion by 2025, up from US$86.4 billion in 2018.
- Pre COVID-19, investment in the sector was growing steadily. However, following the first reported COVID-19 death in January 2020, investment in the sector dropped dramatically, and that trend is forecast to continue in the short to medium term.
- Despite this, 84% of Australian survey respondents indicated their intention to raise capital in the year ahead, signalling optimism in the Australian digital health sector.
- Australian digital health technology development focuses on a diverse set of technologies, including data analytics and systems (25%), mobile-health (22%), AI and machine learning (14%), platform as a service (11%), connected devices and wearables (10%), and telemedicine and telehealth (9%).
- Globally, key areas which are positioned for greater growth due to COVID-19 include telemedicine, remote monitoring, symptom checkers and triage tools, digital therapeutics, tools for expediting drug discovery and clinical trials, and clinical decision support technologies.

Given the opportunities for growth in these technologies, key regulatory issues for companies in this sector will concern data management and regulation of software as a medical device under the Australian therapeutic goods regime. Companies that are able to navigate these frameworks will be well placed to accelerate growth both during and after the pandemic.

The rise of telehealth

Telehealth (including telemedicine) has received particular attention during the COVID-19 pandemic. The forced uptake of the technology by many medical professionals and their patients appears to have resulted in a greater acceptance of digital technology as a means of delivering healthcare services, so much so that its use is predicted to continue well after the pandemic has subsided.

However, before the pandemic, telehealth services were not included on the Medicare Benefits Scheme (**MBS**). Apart from the negative financial impact for patients, some commentators believe that the failure to place telehealth on the MBS has been a disincentive for investment in the sector, thereby stifling innovation.

As an emergency measure during the pandemic, a range of telehealth services were included on the Medicare Benefits Schedule from 30 March 2020 (see list here). These changes are temporary and designed to help reduce the risk of community transmission of COVID-19 during the pandemic (they are currently due to expire on 30 September 2020). However, given telehealth is likely to become a routine method of facilitating healthcare, there are now calls for the placement of telehealth items on the MBS to be permanent. If such a change is made, it could have a significant impact on the growth of the digital health sector in Australia.

Any increased uptake in telehealth will bring into sharper focus the need for GPs, specialists and allied health service providers to ensure that the systems they use to store patient data are secure, and that their remote working information handling practices comply with applicable privacy laws. Digital health technology providers will also need to ensure that their systems are secure and privacy law compliant, including the systems and practices of their

third party infrastructure providers. Compliance with accepted information exchange protocols and integration with MyHealthRecord will also be key.

Telehealth also makes it easier for medical practitioners to conduct inter-jurisdictional patient consultations (i.e. consultations not conducted in person, where the patient or the practitioner is located outside Australia). The Medical Board of Australia requires that medical practitioners using technology to provide inter-jurisdictional medical consultations or services to patients in Australia:

- be registered with the Medical Board of Australia, regardless of where the practitioner is located;
- consider the appropriateness of a technology-based consultation for each patient's circumstances;
- comply with the requirements of the Health Practitioner Regulation National Law (the **National Law**) as in force in each State and Territory of Australia; and
- comply with the Medical Board of Australia's registration standards, codes and guidelines including the Professional Indemnity Insurance Registration Standard, which requires that a medical practitioner is insured for all aspects of their medical practice.

Software as a Medical Device (SaMD)

Different types of digital health technologies attract different levels of regulatory oversight.

Software which meets the definition of 'medical device' under section 41BD of the *Therapeutic Goods Act 1989* (Cth) (**SaMD**) must be registered on the Australian Register of Therapeutic Goods before it can be supplied. Examples of SaMD include:

- mobile apps coupled with devices that calculate insulin doses based on a person's blood glucose levels;
- x-ray image processing software; and
- software that uses information about symptoms to make a diagnosis.

In addition to telemedicine, remote monitoring technology is seen to have significant growth opportunities in a post-pandemic world. Given that a device used to monitor a body function will be a medical device under the Therapeutic Goods Act, the impact of regulation under the Therapeutic Goods Act should be considered in the early stages of product development and will be a significant part of the commercialisation pathway for these technologies.

The regulation of SaMD has been a key focus of the Therapeutic Goods Administration (**TGA**) over the last few years due to the inadequacy of the legislation to keep pace with advances in technology (we wrote about this in detail here). The consultation process has resulted in new regulations which will come into force on 25 February 2021. The TGA has set out a summary of the changes here.

Compliance with the Australian Consumer Law

Any digital health technology delivered to Australian consumers must also comply with the Australian Consumer Law (**ACL**). This includes a statutory guarantee that the technology will be of acceptable quality (including that it will be fit for the purpose that the supplier said it would be fit for).

The ACL also prohibits a supplier from making false or misleading representations (e.g. representations about the performance of the technology where the supplier does not have a reasonable basis (e.g. sufficient clinical evidence) to support the representations). In addition, unfair contract terms must not be included in any standard form agreement that individual consumers may be required to agree to before they can use the technology.

A supplier cannot exclude the application of the ACL to its contracts with consumers (e.g. by making the user terms subject to the laws of a foreign jurisdiction). Compliance with the ACL needs to be carefully managed, but doing so will assist to build a supplier's reputation and trust amongst users, which will be critical to user uptake in the digital health sector.

Digital medical technology in a post COVID-19 world

While COVID-19 accelerated the use of digital medical technologies in some respects, it has also presented significant challenges.

The technological innovation necessary for success in the digital health sector requires access to capital and the traditional capital sources have generally been constrained due to COVID-19. Companies looking to foreign investment to support their growth will also need to be aware of the changes to the FIRB processes, implemented in March 2020 in response to COVID 19 (see our article on this topic here) and the permanent changes expected to be implemented in early 2021 (see our article on this topic here).

Regardless of the regulatory and financial constraints, there appears to be significant optimism in the digital health sector. If made permanent, the newly-introduced Medicare reimbursement of telehealth services may also foster further innovation, opportunity and growth in the sector.

Australia's security monitor recommends changes to controversial 'anti-encryption' legislation

By Philip Catania, Partner, Michael Do Rozario, Partner, Phillip Magness, Lawyer and National Forensic Technology Manager and Rachael Pluta, Lawyer

In December 2018, the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (**TOLA Act**) was enacted. An omnibus Act, the legislation included amendments to the *Telecommunications Act 1997* (Cth) (**Telecommunications Act**), granting new powers for law enforcement and intelligence agencies to obtain information and industry assistance from Designated Communications Providers (**Providers**).

There has been polarising commentary on the TOLA Act, with it being dubbed as Australia's 'anti encryption law'. On the one hand, concerns have been raised over the 'serious threats' that the TOLA Act poses to 'cybersecurity, privacy and freedom of expression in Australia and around the world',[1] and on the other, the view that 'the true danger is the thing the TOLA Act seeks to prevent: terrorists, paedophiles and other criminals communicating in secret, without law enforcement and security agencies being able to 'crack their code''[2]

In March 2019, the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) requested that the Independent National Security Legislation Monitor (**INSLM**), Dr James Renwick SC, review the TOLA Act. The INSLM was required to report on whether the TOLA Act:

- contains appropriate safeguards for protecting the rights of individuals;
- remains proportionate to any threat of terrorism or threat to national security, or both; and
- remains necessary.[3]

The INSLM report was submitted to the Attorney-General on 30 June 2020 and publicly released in a 316-page report last week.[4] A key recommendation was that the process to authorise compulsory orders must be made by a technically informed decision-maker who was independent of the Government agency that would utilise the power once granted.

This was considered to be a missing factor to ensure proportionality and human rights protection in both perception and practice. To ensure this independence, the INSLM recommended the power be removed from the agency and the Attorney General and vested in an Investigatory Powers Commissioner (**IPC**) within the Administrative Appeals Tribunal (**AAT**).

1 Human Rights Watch, *International Civil Liberties and Technology Coalition Comments on the PJCIS Review of the Assistance and Access Act, 2018*, view here.

2 Australian Signals Directorate, *Director-General ASD statement regarding the TOLA Act 2018* view here.

3 Independent National Security Legislation Monitor, *Review and Report of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act* 2018, view here.

4 The full report is available here.

A quick revisit of the powers under the TOLA Act

The TOLA Act introduced three types of industry assistance powers, differing in their coercive nature. As we have covered in a previous article, the primary powers can be summarised as follows:

Request / Notice	Description
Technical Assistance Request (**TAR**)	A voluntary request for a communications provider to assist the Australian Security Intelligence Agency (ASIO), Australian Secret Intelligence Service (ASIS), Australian Signals Directorate (ASD) or an interception agency[5] The Provider may use their existing capabilities or build a new capability
Technical Assistance Notice (**TAN**)	A compulsory notice requiring the communications provider to assist ASIO or an interception agency. The assistance is limited to the use of the Provider's existing capabilities and cannot be used to build a capability the Provider does not have
Technical Capability Notice (**TCN**)	A compulsory notice requiring the communications provider to build a new capability. Once built, ASIO or an interception agency can seek assistance under an issued TAN

Broadly applied, a request or notice can be issued to a Provider, which includes any company, business or person who contributes to the communications supply chain in Australia. A website owner, for example, could be bound by the TOLA Act. Non compliance may result in civil penalties of approximately A$10 million for a corporation and $50,000 for an individual.[6]

The INSLM's recommendations for change

The INSLM largely accepted as valid the following three key criticisms of the TOLA Act:[7]

- the absence of independent authorisation for the compulsory notices (TANs and TCNs);
- the inadequacy in the definitions of some key technical terms; and
- the absence of independent technical assessment of proposed notices.

The 12 key recommendations for change were as follows:

Recommendation 1 – Expansion of powers to integrity agencies.

Currently, the power to issue a request or notice is limited to intelligence and interception agencies and the Attorney-General. However, integrity and anti corruption agencies 'face the same challenges in fulfilling their mandate as a consequence of the growth in encryption of communications as do police'.[8] As these agencies are already empowered to exercise various investigative powers under other legislative schemes (e.g. the power to make requests under s 313 of the Telecommunications Act), the INSLM recommended that the reach of the TOLA Act be extended to integrity and anti corruption agencies.[9] This will include the Commonwealth Integrity Commission, if it is subsequently established.

Recommendation 2 – No change to Technical Assistance Requests.

As a TAR is not a coercive instrument, the INSLM did not recommend any changes to the existing TAR arrangements, except for the use of a prescribed form.[10]

5 An interception agency is the Australian Federal Police (AFP), Australian Criminal Commission (ACIC) or a State or Territory police force.
6 A notice to an individual occurs in the context of a sole trader and not to the employees of a corporation.
7 Independent National Security Legislation Monitor, Parliament of Australia, *A Report Concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (2020) (Report on the TOLA Act) [1.24].
8 Ibid [10.49].
9 Ibid [10.44], [10.49].
10 Ibid Act [1.64], recommendation 2

Recommendation 3 – Changing the authorisation for compulsory notices.

The report noted the near unanimous concern from non-Government stakeholders over a lack of an independent authorisation process for TANs and TCNs. The INSLM did not accept the Government's submission that effective and sufficient oversight mechanisms existed. Rather, the INSLM considered that the authorisation of coercive statutory powers without independent review must only occur in exceptional and justified circumstances.

As the INSLM considered, '[a]ny scheme involving the use of coercive statutory powers must ensure that it has the necessary checks and balances to ensure not only that correct and lawful decisions are made but also that they are seen to be made'.[11] The INSLM highlighted the importance of instilling and inspiring trust in the community for the decisions that are made.

The INSLM recommended that TANs and TCNs should be authorised by a body with access to technical advice that is independent of the issuing agency or Attorney General. Accordingly, the INSLM recommended that the powers to issue the compulsory order vest in the AAT and assigned to a newly created Investigatory Powers Division (**IPD**).

Recommendations 4 to 6 – Establishment of the Investigatory Powers Division and Investigatory Powers Commissioner.

The INSLM recommended the creation of a new IPD within the AAT with powers and procedures that build on the existing Security Division.[12] The IPD would use existing AAT powers, conduct private hearings and alternative dispute resolution, receive submissions from both the agency and the Provider, possess the expertise to resolve technical questions and ultimately determine whether a TAN or TCN should be issued.

The IPD is conceptually based on the United Kingdom's Investigatory Powers Commissioner's Office, however differences exist.

The INSLM recommended that the IPD be comprised of an IPC and other eminent lawyers and technical experts as needed. The IPC should be a retired Federal or Supreme Court judge. Importantly, the INSLM found that the power to determine a TAN or TCN should remain with the AAT as a statutory office as there are fundamental difficulties in vesting such a function in a court. These difficulties were principally based on the public nature of court hearings such that difficulties may be present in limiting access to a Provider's highly sensitive commercial-in-confidence information and the secret and operational information of the Government.[13]

Recommendation 7 – Definitions of 'serious Australian offence' and 'serious foreign offence'.

The industry assistance powers introduced by the TOLA Act may be exercised in relation to a 'serious Australian offence' or a 'serious foreign offence'. Under the Telecommunications Act, a serious Australian or foreign offence is punishable by a maximum term of imprisonment of three years or for life.[14] The INSLM found that this three year threshold captures a range of less serious offences, rather than the offences for which the industry assistance powers were sought to be made available (e.g. terrorism and child sex offences).[15]

The INSLM recommended that the threshold be aligned to s 5D of the *Telecommunications (Interception and Access) Act 1979* (Cth) in which a serious offence is one on a proscribed list, an offence punishable by life imprisonment or an offence carrying a term of at least seven years imprisonment.

Recommendations 8 to 10 – Amendments to key definitions including 'systemic weakness'.

Arguably, one of the most controversial and publicly debated aspects of the TOLA Act is that a request or compulsory order must not have the effect of:

- requesting or requiring a Provider to implement or build a systemic weakness, or a systemic vulnerability, into a form of electronic protection; or
- preventing a Provider from rectifying a systemic weakness, or a systemic vulnerability, in a form of electronic protection.[16]

What is allowed is for a weakness or vulnerability to be introduced to a 'target technology' that only affects an individual person (e.g. perhaps by way of introducing a security flaw in a mobile phone application that affects one user only). The provisions have been criticised for lack of clarity, breadth and practical application, and for potentially requiring subjective or arbitrary application.

The INSLM recommended a number of changes including:

- removing the definition of 'systemic vulnerability' as the term was not conceptually different to 'systemic weakness;
- clarifying the definition of a 'target technology' through the use of non exhaustive statutory examples of what is included (e.g. a particular device or mobile number for one target only) and what is to be excluded;
- amending the definition of 'systemic weakness' to bring it in line with the submissions received from industry;
- amending other key definitions; and
- where a weakness is selectively introduced, re-drafting the provision relating to limitations with a focus towards an assessment of material risk.

11 Ibid [10.9].
12 Ibid [11.1].
13 Ibid [11.9].
14 Telecommunications Act s 317B.
15 Report on the TOLA Act [12.33] – [12.35].
16 TOLA Act s 317ZG(1).

Recommendation 11 – Removal of reference to a natural person.

The INSLM recommended that the definitions of a Provider should not be taken to include a natural person who is an employee of the Provider. This potentially removes a scenario where an individual employee may be issued a notice personally that may limit certain protections. The INSLM made it clear that a natural person should only apply to an individual who is a sole trader.

Recommendation 12 – Reduced role for the Australian Federal Police.

Presently under the TOLA Act, the AFP Commissioner must approve a TAN that is requested by the police force in a State or Territory.[17] The INSLM has recommended that AFP approval is no longer required.

What happens next?

Following the release of the report, the Attorney-General acknowledged the work of the INSLM and confirmed that the Government will carefully review the report's recommendations and the outcome of a PJCIS review which is due in September 2020.[18]

Although it is not likely that the Government will move to amend the TOLA Act prior to the review, some of the controversial and presently existing aspects of the TOLA Act may inhibit the Government's ability to enter into a bilateral executive agreement with the United States under the Clarifying Lawful Overseas Use of Data Act (CLOUD Act). Australia's intention to accede to the CLOUD Act follows the recent introduction of the introduced *Telecommunications Legislation Amendment (International Production Orders) Bill 2020* (Cth).

There is also a private members bill, the *Telecommunications Amendment (Repairing Assistance and Access) Bill 2019* (Cth), which was introduced by Senator the Hon Kristina Keneally. This proposes a number of amendments to the TOLA Act, many of which align with those proposed in the INSLM report. The Bill has been before the Senate since December 2019.

Subject to exceptions that can be addressed through change, the INSLM review ultimately concluded that the TOLA Act is, or is likely to be, necessary, proportionate to the security threat faced, and affording the proper protection for human rights.[19] On this basis, and with the Attorney-General reiterating the criticality of the TOLA Act to protect Australia's national security,[20] we suspect that the TOLA Act is likely to remain for the long haul.

17 Ibid s 317LA.

18 Attorney General for Australia and Minister for Industrial Relations, 'Independent National Security Legislation Monitor Report tabled' (Media Release, 9 July 2020, view here.

19 Report on the TOLA Act [1.4] – [1.6].

20 Attorney General for Australia and Minister for Industrial Relations, above n 19

The future of outsourcing in the aftermath of COVID-19

By Arvind Dixit, Partner and James North, Head of Technology, Media and Telecommunications

COVID-19 has exposed weaknesses in the traditional outsourcing model. As the world finds a 'new normal', key learnings from the pandemic are likely to shape the way organisations approach their outsourcing arrangements into the future.

While COVID-19 has impacted the entire global economy, organisations that have outsourced core business and operational functions have been particularly exposed, one example being the impact that lockdowns in India and the Philippines have had on Telstra to deliver on new orders and manage faults. The full extent of the impact of the pandemic on outsourced operations is not yet known, and infection rates in a number of countries that support large Business Process Outsourcing (**BPO**) sectors do not yet appear to have peaked.

Aspects of the traditional outsourcing model have been proven to be flawed, and organisations now have an opportunity to build more resilient frameworks to protect against similar occurrences. An organisation's outsourcing and supply chain strategy has greater C-suite and board attention than in the past, and there will be an expectation on GCs and legal teams to be familiar with these strategies, and to ensure that the organisation adopts appropriate risk mitigations to enable it to survive future pandemics and other black swan events. The following areas warrant consideration in the context of future outsourcing arrangements.

1 Business continuity and disaster recovery.

Historically, business continuity planning (BCP) has been underpinned by a requirement to have a multiple physical backup sites that are capable of being quickly deployed in the event of an incident. This generally assumes that workers and systems at one location can be easily transitioned to another location (often in close geographic proximity) in order to ensure continuity.

This is particularly prevalent in the context of BPO arrangements which are heavily reliant on remote workforces. Although multiple physical locations is an important part of BCP and disaster recovery, this will not provide effective protection in the context of a broad global lockdown, as COVID-19 has demonstrated. Moving forward, organisations will need to be comfortable that their business continuity planning includes mechanisms to deal with broad-based remote working, and that these mechanisms have been, and are capable of being, stress tested on a regular basis.

2 Remote working as the 'new normal'.

It seems increasingly likely that some form of remote working arrangements will be in place for the foreseeable future. This reality heightens the importance of organisations incorporating appropriate information and data security requirements into their outsourcing arrangements. Often, security mechanisms associated with remote workforces have been focused on physical security (e.g. physical access control to secure sites). In a remote working environment, the focus will need to include logical security mechanisms (e.g. electronic access control and technical controls to prevent exfiltration of information to private systems).

Organisations will also need to have appropriate mechanisms in place to control the level of performance of their service provider's workforce when physical supervision is not possible. This might include requiring service providers to electronically monitor the quantity of output of individuals, or to structure arrangements to be output driven (as opposed to time and materials based) so that the delivery risks, and risks associated with potential reduced efficiency in a remote environment, are shifted to the service provider. We expect that organisations will require their service providers to provide a detailed plan (which has been, and is capable of being, stress tested on a regular basis) setting out how remote working will be implemented, and how performance risk will be managed when physical supervision isn't possible.

3 Broad review of outsourcing strategy.

One of the key benefits of outsourcing business functions is the potential to tap into a skilled workforce in a country with a lower cost base (particularly where there is a skills gap in the home jurisdiction). The obvious risk of this is that it diminishes the level of control an organisation might exert over the remote workforce, and it relies on a seamless communication and mobility of information and resources. While the cost benefits of outsourcing will always be a major attraction, there is an increased focus on supply chain robustness and resilience. We commented on this in further detail in an earlier piece. This is now a C-suite issue with board scrutiny, and is likely to necessitate broad reviews of the outsourcing strategy of organisations, particularly in relation to critical functions. We expect organisations to pay close attention to whether critical functions which may have been outsourced can be brought in-house or on-shore.

We also expect to see an acceleration of investment in automation of labour-heavy activities to reduce the dependence on human capital (and therefore the susceptibility to pandemics or other health issues). This flight to automation and 'bots' during the pandemic has already been evident amongst organisations with substantive outsourced operations. Increased use of automation in outsourcing may be an opportunity to bring functions back on-shore while managing the cost of doing so to a reasonable level. There is also likely to be an acceleration of cloud migration given the flexibility that cloud computing offers to scale up and scale down operations to cope with external demand shocks caused by pandemics and similar black swan events.

4 'Big bang' BPOs may be a thing of the past.

Building on point three above, we expect organisations to consider moving away from single-source models for particular critical functions which would benefit from being multi-sourced from vendors in a range of different geographic locations, each of which is capable of 'stepping in' if another vendor is incapable of performing. The benefits of a single-source approach are twofold. Firstly, the customer negotiates a low overall price and secondly, the customer has a single point of contractual accountability (the so called "single throat to choke"). The result has often been that the service provider uses the lowest cost/offshore location, sometimes to the detriment of the customer from a quality and risk perspective. Also, the supply chain becomes opaque and the customer is unaware of how the service provider will perform in the event of a pandemic or other black swan event. The benefits of a single-source model need to be carefully weighed against the lack of supply chain resilience and the inherent exposure that this brings.

5 Re-thinking governance and control structures.

Strong governance processes and mechanisms are often key to the successful implementation and operation of outsourced arrangements. These processes rely on having shared working spaces, physical meetings and gatherings, or in the case of remote workforces, the constant presence of representatives of the organisation at the premises of its service provider and vice-versa. The concept of physical proximity is particularly relevant in an agile delivery context that depends on the close and continued interaction of team members. Organisations will need to re-think the way that traditional governance models can effectively operate in a remote working context.

One of the trends that became evident in the early stages of COVID-19 was that organisations were forced to relax some of their stringent governance arrangements in order to accommodate the changed work environment. Being nimble in this context was a benefit to these organisations. However, there is a clear balance that needs to be struck between loosening governance, and completely removing governance and control structures. It would be beneficial for organisations to have a tiered structure of governance and controls that can be easily ratcheted up or down depending on the circumstances, and which has been pre-determined and stress tested in the context of a remote working environment.

6 Increased contingency planning of the 'worst case'.

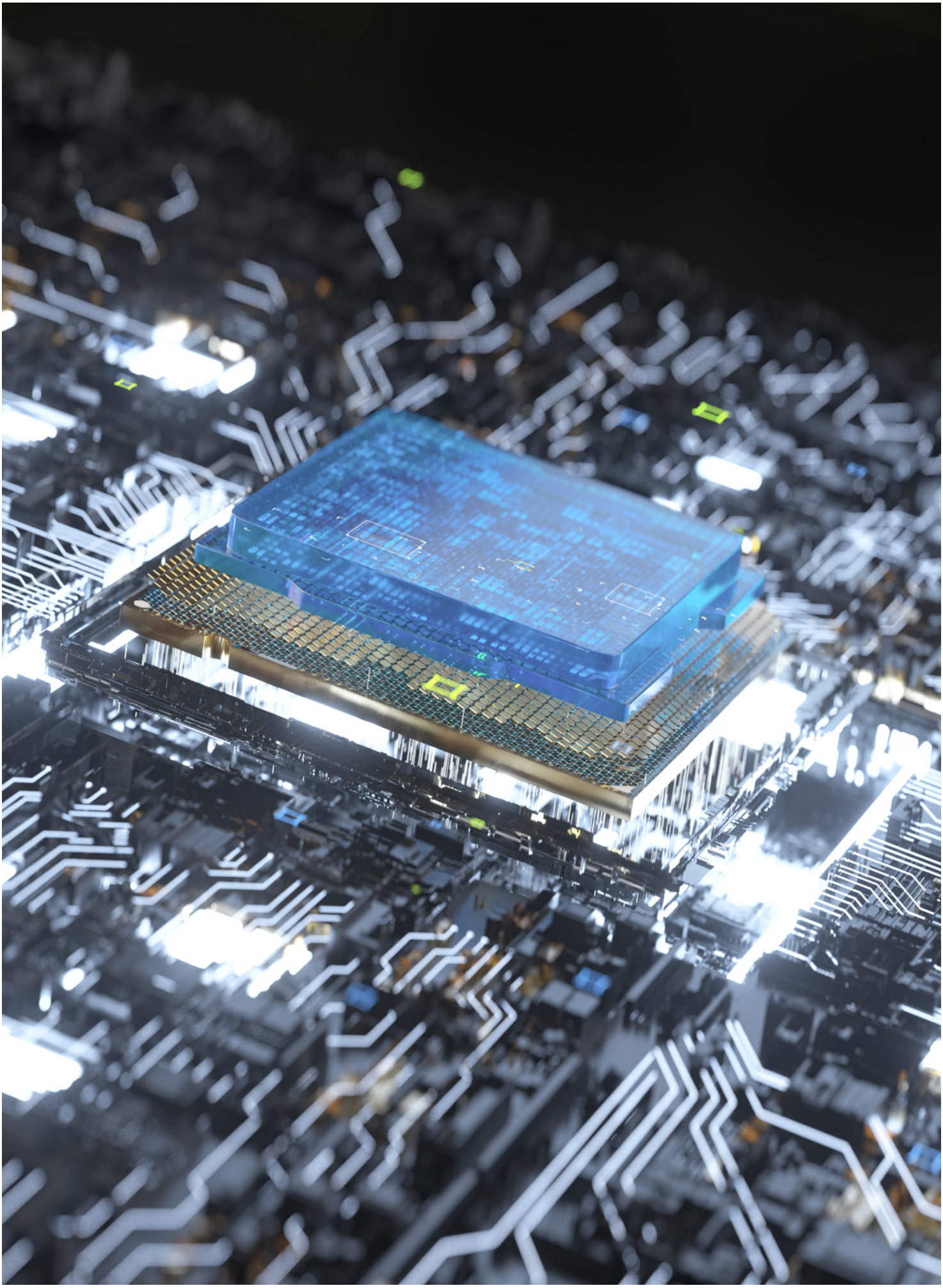
At the beginning of the pandemic, there was a flurry of activity in relation to the application of existing force majeure clauses or 'frustration' based arguments to the present circumstances. Where it could be said that occurrence of COVID-19 constituted a force majeure event, often the impact was the service provider being relieved of its contractual obligations. From a customer perspective, a more desirable outcome is a potential relaxing of obligations to an agreed baseline of performance, rather than a complete release from all obligations.

We expect to see a heightened focus on contingency planning (even in the context of low probability, high impact events), which then translates into variable performance obligations and pricing structures which are hard-coded into the outsourcing arrangement so that there is complete clarity on performance and price expectations if a similar event occurs. We also expect that organisations will require potential service providers to provide details of their "worst case" modelling when responding to tenders in large scale outsourcing projects.

Although COVID-19 has had a significant impact on outsourced arrangements in the short term, we expect to see strong and sustained demand for outsourced services in the longer term as part of accelerated digital transformation activities within organisations. By considering and addressing the points above, organisations will be able to increase the resilience of their outsourced arrangements. GCs and legal teams have an important role to play in helping to guide this thinking.

To watch a short video on this topic on the Corrs website, click here.

This article is part of Corrs' insight series COVID-19: Navigating the implications for business in Australia and beyond. To get notified by email when new COVID-19 insights are released, please subscribe for updates here.



Open banking, 'big data' and AI: what are the implications for the financial services sector?

By James North, Head of Technology, Media and Telecommunications, Felicity Healy, Partner and Jennifer Dean, Special Counsel

Access to large consumer data sets is increasingly driving new and innovative ways of doing business for traditional banks and fintech startups, whether it be the use of artificial intelligence (AI) tools to determine credit eligibility or the design of novel services relating to budgeting, investment tracking or deferred payments.

With cash transactions decreasing, COVID-19 accelerating the move away from face-to-face interactions in local branches and the Australian implementation of 'open banking' – which gives consumers the right to transfer their transaction and account data between banks – such innovations are only set to continue.

The interplay between this trend and financial services regulation is dynamic, and it is reasonable to expect that the use of 'big data' by financial services providers will attract greater attention from regulators including ASIC, the ACCC and the OAIC in future.

Open banking in particular will provide lenders with significant inflows of reliable transaction data about prospective customers. This is likely to drive more sophisticated consumer offerings, including greater personalisation of financial services and has a number of significant implications for lenders.

Under consumer credit legislation, credit providers must assess whether a product is suitable for a particular customer having regard to reasonably available information about the consumer's financial situation. Where a lender fails to request consumer data under the open banking framework or fails to properly consider data it receives, it may breach its responsible lender obligations.

Banks already have policies in place to assist with the assessment of whether someone is likely to experience substantial hardship as a result of obtaining credit. However, in the context of open banking and the ability to access greater amounts of reliable information, these policies and procedures will need to be refined.

Systems may also need to be redesigned to ensure that red flags are triggered for certain types and amounts of spending (such as the frequency and amount of money spent gambling). In future, issues are particularly likely to arise in circumstances where the open banking data indicates that credit is unsuitable, but traditional verification methods (such as self-reported expenses) suggests otherwise.

Similarly, access to open banking data may have implications for financial services providers in terms of their compliance with anti-money laundering and counter-terrorism funding reporting obligations.

Access to the increasing volumes of consumer data which will be available to financial services institutions through open banking may result in an accelerated use of AI in credit decision-making. While these tools undoubtedly have great potential, proper design and oversight is critical to ensure they do not perpetuate unconscious bias or discrimination against certain customer demographics. This issue is the subject of an ongoing review by the Australian Human Rights Commission which released a substantial discussion paper on Human Rights and Technology at the end of last year.

Managing open banking data is also likely to present a number of data governance challenges. Open banking data is subject to significantly stricter privacy safeguards than those that apply under general privacy law, and financial services providers will need to implement systems and access controls that can effectively manage the different protocols for the collection, storage and use of the different kinds of data they hold.

Maintaining appropriate access controls is becoming both more complex and critical over time. Unsurprisingly, there is an increasing regulatory focus on these issues, and 2019 saw the OAIC secure court enforceable undertakings from financial institutions to rectify deficiencies in this regard.

Big data and open banking present real opportunities for innovation and increased competition in the financial services sector, but they also create a number of challenges for both banks and fintechs in terms of their broader data governance practices and regulatory compliance.

5G investment in Australia: challenges and opportunities in the Australian market

By Eddie Scuderi, Partner and Ross Allen, Lawyer

The advent of fifth generation mobile technology (5G) is set to create significant challenges and opportunities for stakeholders in the telecommunications industry.

The transition to 5G will lower the cost of delivering data for mobile network operators (**MNOs**) and will also provide Australian mobile consumers with a higher quality of service which will allow MNOs to meet the demands for new and emerging data-driven services.

However, reaching this point will require significant investment from MNOs, such as building more mobile towers, cells and acquiring new spectrum to ensure that they can support the delivery of 5G and maximise its capabilities.

The challenge for the Australian Federal Government and regulators will be striking a balance between incentivising investment and facilitating a competitive landscape that will benefit Australian consumers.

This article examines the challenges and opportunities that lie ahead for investment and the regulation of the telecommunications industry in Australia.

Investment in the Australian 5G rollout

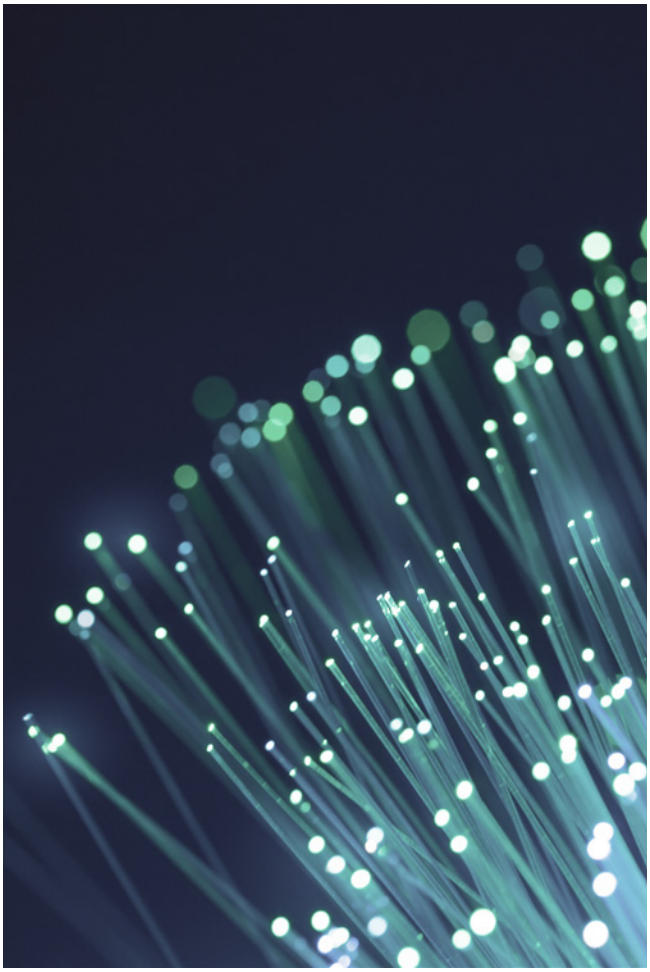
The mobile telecommunications sector in Australia is currently preparing for a generational shift that will see significant advances in technology. Although the benefits this transformation will have on industry and innovation in Australia are largely yet to be realised, what is apparent is that the future of 5G promises to provide high data speeds, high reliability and low latency.

To help achieve the rollout of 5G, the Government has outlined a number of policy objectives and law reforms to support network deployments. In its 2017 directions paper, 5G – Enabling the Future Economy, the Government identified its objective to support the rapid deployment of 5G networks by ensuring that spectrum is made available in a timely manner and that arrangements are made which will allow MNOs to deploy the necessary infrastructure quickly.[1]

In line with these objectives, the Government recently legislated its spectrum re-allocation declaration,[2] which allows the Australian Communications and Media Authority (**ACMA**) to re-allocate ultra-fast millimetre wave 26 GHz band spectrum (**mmWave**) across 29 regions in 2021. The Government stated that making this new mmWave spectrum available will assist MNOs in rolling out the network and providing extremely fast high capacity services.[3]

Although MNOs support the allocation of these high frequency mmWave bands, the allocation of more spectrum in lower frequency bands is also required. This is in part because high-frequency spectrum, such as the mmWave bands, have propagation limitations, including reduced range and low indoor penetration.[4]

1 Department of Communications and the Arts, *5G – Enabling the Future Economy*, p 10.
2 Radiocommunications (Spectrum Re-allocation—26 GHz Band) Declaration 2019.
3 Australian Government, Department of Communications and the Arts, Communications Policy Objectives for Allocation of the 26 GHz band, available here.
4 McKinsey and Co, The Road to 5G, the Inevitable Growth of Infrastructure Costs, available here.



Although the Government has highlighted its commitment to assist MNOs with the successful deployment of the network, the fast and efficient rollout of 5G across Australia still depends heavily upon MNOs making costly infrastructure investments. Even after MNOs acquire new spectrum, additional physical infrastructure is still required to supplement the network so it can achieve the coverage and usage that it is capable of delivering. To overcome these limitations, MNOs must install new towers and also retrofit new cells across major cities.[5] Network costs have also been projected to double as MNOs manage the upgrade from 4G to 5G.[6]

These challenges will make it more difficult for MNOs to maintain their profitability in the short to medium term while their networks are being rolled out. For this reason, the Government and regulators must work in tandem to support the investments being made by MNOs for the success of the network.

Regulating MNOs and the network in the emerging 5G market

In light of the significant challenges and costs that MNOs face in rolling out 5G, it is important that regulatory settings do not hinder fast and cost-effective rollouts of this critical infrastructure.

In its 2019-2023 five year spectrum outlook (**FYSO**),[7] ACMA recognised the importance of ensuring spectrum is made available to MNOs in a timely manner.[8] ACMA has also stated that information about the timing and sequence of major spectrum allocations will be provided in advance under its forward allocation work program.[9] This is to ensure that both prospective and incumbent spectrum licence holders can make informed and strategic decisions to better support their network planning and manage their investment costs.[10]

To facilitate effective rollouts, ACMA will also need to balance the new and emerging approaches to sharing spectrum which could improve the network for consumers, with the need for certainty of investment for existing and incumbent spectrum licence holders. ACMA has noted in its FYSO that maximising the use of spectrum may involve implementing new sharing techniques that have been developed, such as dynamic spectrum access (**DSA**).[11]

DSA is an approach to sharing access to spectrum, where lower-tier users dynamically give way to higher-tier users depending on their demands at given times.[12] International telecommunications regulators such as the Federal Communications Commission (**FCC**) in the United States and the Office of Communications (**Ofcom**) in the United Kingdom have started looking into the appropriateness of transitioning their networks to a model of this kind.[13]

To continue reading this article on the Corrs website, click here.

5 Infrastructure Australia, *Australian Infrastructure Audit – Telecommunications 2019*, p 572.
6 McKinsey and Co, The Road to 5G, the Inevitable Growth of Infrastructure Costs, available here.
7 Australian Communications and Media Authority, Five-year spectrum outlook 2019–23 The ACMA's spectrum management work program.
8 Ibid, p 53.
9 Ibid, p 53.
10 Ibid, p 53.
11 Ibid, p 20.
12 Ibid, p 20.
13 Office of Communications, *Enabling wireless innovation through licensing, shared access to spectrum supporting mobile technology*, July 2019.

Technology procurement challenges for 'smart building' developers and operators

By Daniel Thompson, Special Counsel and James North, Head of Technology, Media and Telecommunications

State of the art 'smart building' technology has rapidly become a key differentiator for all stakeholders in the real estate value-chain – owners, operators, tenants and end users. However, as building technology becomes more complex, building developers and operators face new challenges that require technology-specific skill sets to address.

The data-driven 'smart buildings' of tomorrow will be made possible by the core technologies of Industry 4.0 – namely, 5G, IoT, AI and cloud. They will offer unprecedented customisation and control, operational efficiencies and cost saving, and will also generate valuable data sets. Smart building technology will use fleets of IoT sensors, machine learning and data analytics to learn occupant preferences, monitor occupant activity, connect physical and electronic identity, provide digital design tools, and automate 'operational' building technology (e.g. climate control, lighting, fire, and security).

COVID-19 has brought many of the benefits of smart buildings into acute focus: automated and remotely managed building systems have minimised the need for onsite staff during lock-down, and technologies such as thermal cameras, occupancy monitoring systems and dynamic space allocation management offer innovative solutions to safely return to work. However, with these benefits come a number of new challenges that require technology-specific skill sets to address, for example:

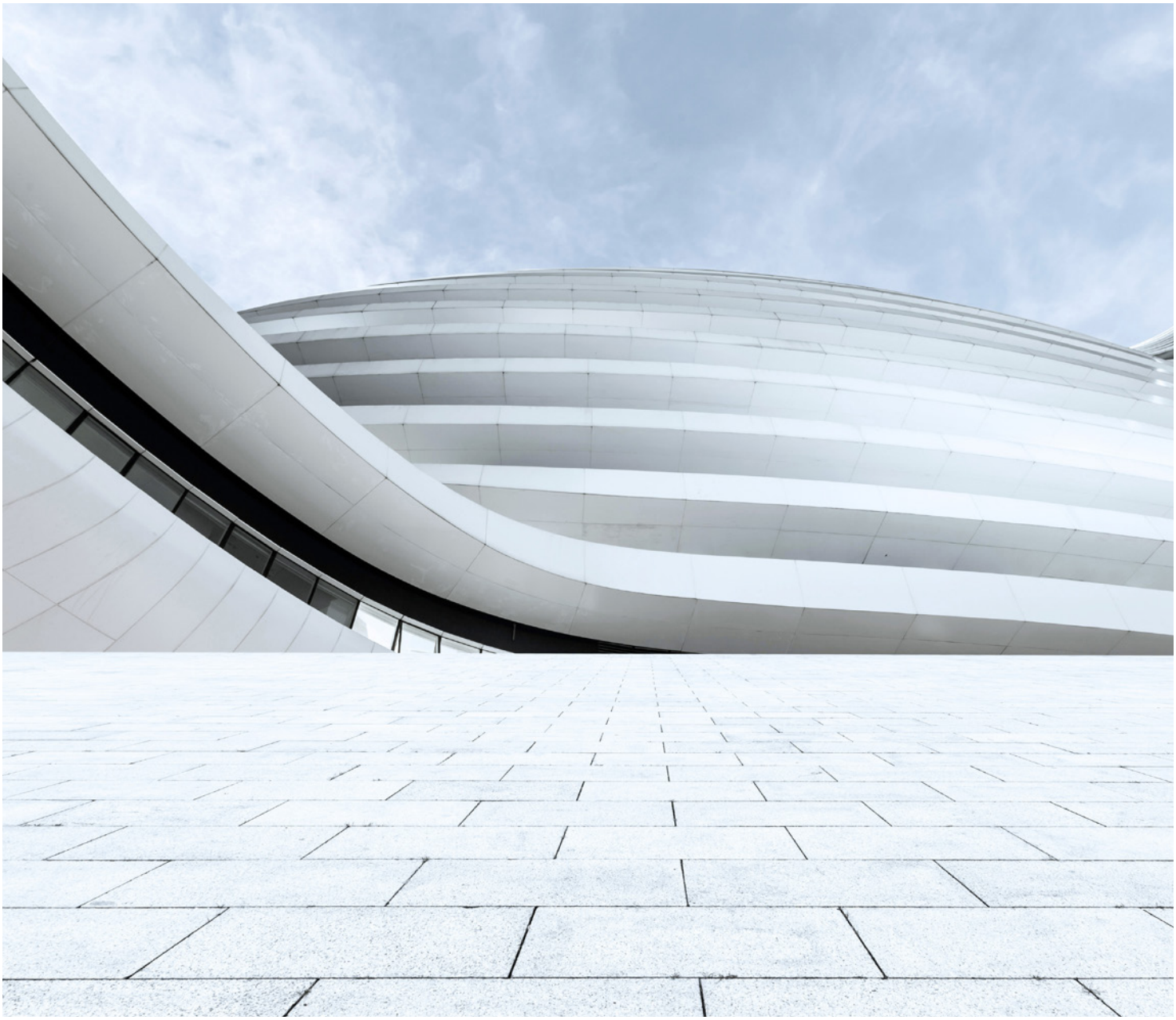
- IoT devices used in smart buildings, and their connection to various cloud environments, present a far greater attack area for hackers to gain access to building systems, and the interconnectedness of building systems will increase the risk of harm that may be caused by cyber breaches;
- the data sets generated by smart building sensors and analytics systems are likely to contain personal information of individual occupants or visitors and will require rigorous attention at the design stage and ongoing controls to ensure privacy compliance; and
- the design, integration and lifecycle management of smart building technology will involve an increasing number of vendor solutions and greater complexity to manage internally.

Many developers and operators will not have the internal capability to address these challenges and, for this reason, procurement and management of smart building technology is increasingly outsourced to specialist building technology contractors, or 'Master Systems Integrators' (MSIs). However, the procurement approach to (and commercial and contractual model for) engaging an MSI is not well established.

Traditionally, building developers have contracted numerous technology vendors for a range of particular building systems, generally under the head building contractor and after the building planning and design stages are complete.

As technology moves from the periphery to the centre of future building design, early engagement with an MSI will be integral to ensuring that technology solutions are adapted to meet business objectives and overall building strategy.

MSI engagements will become far more complex than traditional technology contracts, and will often involve outsourcing end-to-end responsibility for design, build, commissioning, and ongoing management, support and evolution of smart building technology. Developers and operators of smart buildings should be rethinking their procurement and contracting approach to technology implementation in order to reap the benefits promised by smart building technology.



Outcomes-based procurement

The reality of most building systems today is that information is siloed in individual systems. A core aim of smart buildings is to integrate building systems to enable data flows from these systems to be collected, analysed and used in real-time to support desired outcomes. For example, a business objective may be to identify whether a meeting room is occupied. There may be many ways of achieving such an objective, using data from one or more building systems:

- data from a meeting room scheduler may show a room is booked;
- data from a lighting sensor may show that a room is unoccupied; and
- data from workplace tracking systems may show that the scheduled attendees are not in the building, or in another meeting room.

Generally, when procuring smart building technology, developers and operators should focus on developing clear business outcomes or capability 'use cases', rather than prescribing particular technology requirements to achieve these outcomes. This 'business outcomes' procurement approach is well suited to the smart building context, as it allows MSIs to utilise their specialist knowledge of legacy, new and on-the-horizon technology, and design and integration expertise, to propose cost-effective solutions.

This approach will also speed up the time to issue an RFP, and increase the scope for MSIs to innovate and compete to provide the best value solution that meets the required business outcomes.

Engagement model

There is no 'industry standard' model of MSI engagement, and contracts take on a number of forms. However, the MSI engagement model will expand beyond simple consulting services, or delivering integrations between particular building systems, and will often encompass end-to-end responsibility for the design, integration, operation and lifecycle of all building technology systems.

The characteristics of deeper MSI engagement models will generally include:

1 End-to-end design & build responsibility.

The MSI will be responsible for designing and delivering a turn-key technology solution that meets the customer's requirements, including responsibility for ensuring all third party systems incorporated in the solution are fit for purpose. This approach shifts design risk from the developer to the MSI, whose expertise in the vendor market leaves it best placed to recommend the right systems, and removes the opportunity for finger pointing between vendors if requirements are not met. This model of engagement is generally contracted on a fixed-price / fixed-scope basis.

2 Project responsibility.

The MSI will have contractual responsibility for delivering the technology solution to meet a project timetable, and for project managing third party technology vendors and the inputs from the building owner and other stakeholders. In the case of a new construction or renovation, the MSI will need to develop its project timetable around the construction timetable, and work closely with the construction project team to identify design and access requirements. Early engagement in the building design stage is essential for ensuring that the technology and construction projects progress in harmony.

3 Post-commissioning ops.

Traditional facilities management functions will be transformed and in many cases replaced by smart building systems, which require specialist IT and data expertise to operate and maintain that may be beyond the abilities of in-house facilities management and IT teams. Accordingly, MSIs will have a greater role to play in managing the operation of smart building technology than traditional 'operational technology' contractors, which may include IT support and maintenance services, technology vendor management (including management of licensing, vendor software support, and end-of-life issues), cyber security, unified data management, privacy compliance, optimising and improving building operations through data analytics, and training services for in-house teams. A key part of the value MSIs offer in the operational phase of a smart building is to connect building stakeholders to the data generated by building systems in meaningful ways, and assisting operational decision-making based on such data. Performance of such ongoing operational services will be driven by service levels, which may include metrics for systems availability, energy efficiency, preventative maintenance, systems security, and customer satisfaction, among others.

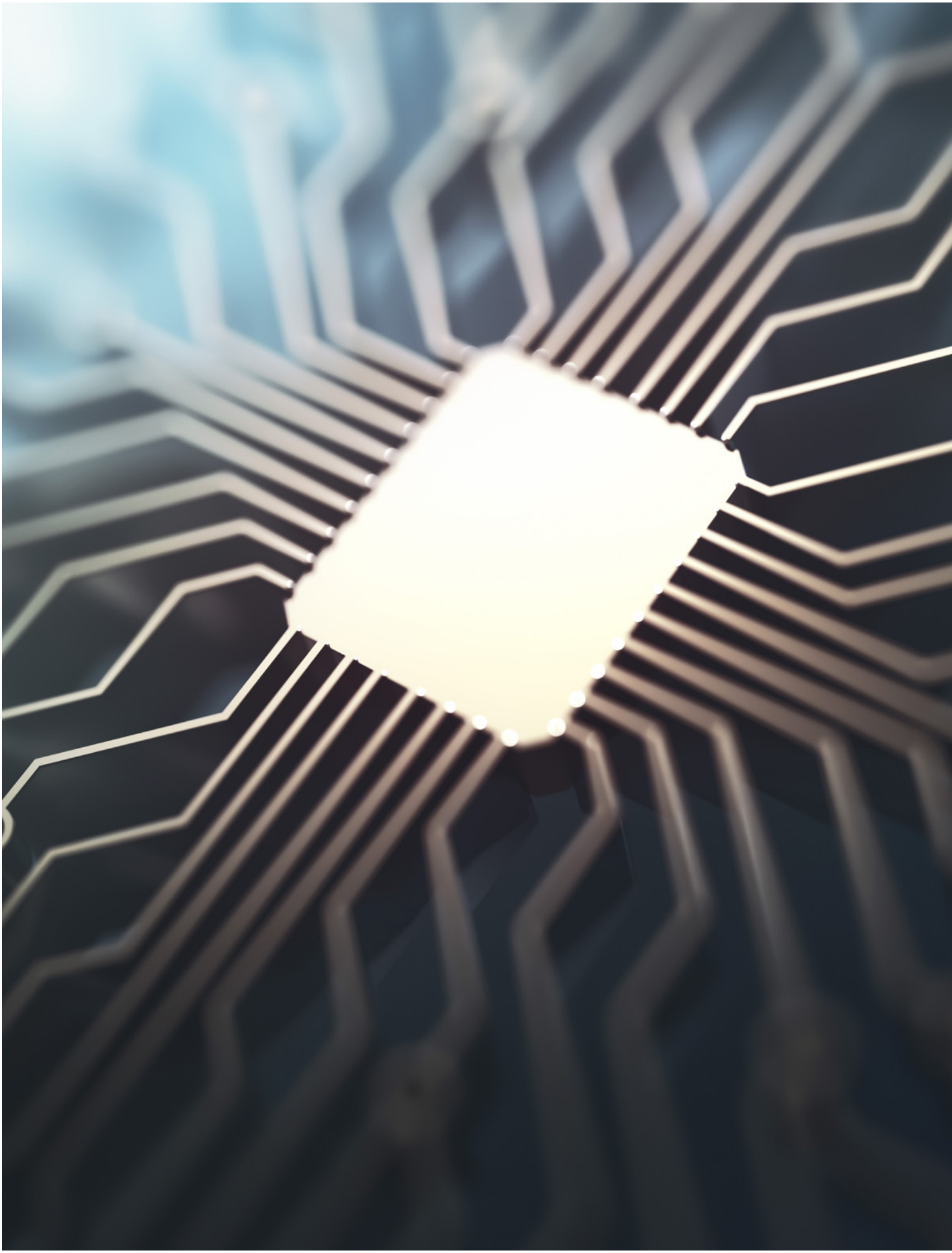
4 Upgrade and enhancement.

Building lifecycles are significantly longer than technology lifecycles, and the technology in smart buildings will evolve in time. In many cases, technology upgrade or enhancement work will commence from the moment the building is commissioned. There is often a gap in perspective between the design and build teams and the stakeholders most invested in the operational use of the building, and this will often result in the MSI development team being engaged in continual development or re-configuration of building systems to meet operational needs. MSI contracts need to contemplate more than the initial solution delivery, and include terms governing how future projects or continuous delivery will be governed. Engagement models may include minor enhancement work built into operations and support services, priced technology roadmap options, gain-share mechanisms for joint investments, and/or agile project development regimes.

Looking ahead

How a smart building owner chooses to engage with a MSI will depend on a number of factors, including the complexity of their technology requirements and their in-house capabilities. Although engagements with MSIs are likely to continue to involve significant consulting work on an hourly rate basis, and piecemeal integration projects, the trend in MSI engagements for truly integrated building systems will shift towards outsourcing end-to-end responsibility for all building technology, both in the delivery and operations stages.

There will always be a cost for pushing greater contractual responsibility on an MSI, but as technology and the smart building industry continues to develop, the value in deeper partnerships with such service providers will become more compelling, and MSIs will become more accustomed to accepting and capable of managing such risk.



Artificial intelligence and copyright: ownership issues in the digital age

By Eugenia Kolivos, Partner, Kate Hay, Head of Intellectual Property and Bethany Lo Russo, Lawyer

In September 2015, the foundations of copyright law were shaken when animal rights group PETA sued British photographer David Slater on behalf of a monkey named Naruto to assert copyright over a 'selfie' taken by the monkey on the photographer's camera.[1]

Although the dispute eventually settled out of court, it raised unique issues about the nature of copyright ownership and challenged the foundational principle that creative works must be authored by a human to attract copyright. As we plunge deeper into the digital age, the concept of authorship is being further muddied in respect of non-human authors – that is, works created substantially or wholly through artificial intelligence (**AI**).

The COVID-19 pandemic has emphasised the need for societies, workforces and even entire nations to mobilise quickly to work. learn remotely and wholly embrace technology. In equal measure, it has emphasised society's commendable ability to do this, as we continue to bear witness to the many creative and collaborative outputs yielded through a time of mass isolation. Creative industries have been hit exceptionally hard by the pandemic, particularly in respect of live performances and television and film production.

In some fortunate cases, these industries have been able to adapt and shift from requiring a physical presence to inhabiting and collaborating in online spaces. As human-to-human collaboration is disrupted by the pandemic, we are seeing a rise in human-to-computer collaboration. As we look towards a post-pandemic world, we anticipate that the role of technology will be elevated even more so. With these drastic technological shifts in mind, this article explores the impacts of artificial intelligence (**AI**) on copyright law, particularly in relation to traditional authorship constructs.

The Australian context

In Australia, copyright subsists in original works which are authored by a qualified person, meaning an Australian citizen or a person resident in Australia.[2] Similar requirements apply in countries all over the world. These global constraints are problematic in circumstances where works are not created through human intelligence but rather through 'artificial neural networks' or 'brain-inspired systems that are designed to imitate the way the human mind learns'.[3]

Indeed, this issue has already been tested to some extent by Australian courts. In *Telstra Corporation Limited v Phone Directories Company Pty Ltd*,[4] the Federal Court found that telephone directories did not attract copyright because they were 'not the result of human authorship but [were] computer generated' and did not involve 'independent intellectual effort' by the human contributors.[5] Likewise, a decade on from this decision, artificial intelligence has come a long way, and computer-generated works are making vast improvements in terms of sophistication and even creativity. Through machine learning, computers are able to absorb vast amounts of creative data, analyse the features and patterns of this data and generate something entirely new.

1 Jason Slotkin, "'Monkey Selfie' Lawsuit Ends With Settlement Between PETA, Photographer', *NPR*, 12 September 2017, available at: https://www.npr.org/sections/thetwo-way/2017/09/12/550417823/-animal-rights-advocates-photographer-compromise-over-ownership-of-monkey-selfie

2 *Copyright Act 1968* (Cth), s 32.

3 Luke Dormehl, 'What is an artificial neural network? Here's everything you need to know', Digital Trends, 6 January 2019, available at: https://www.digitaltrends.com/cool-tech/what-is-an-artificial-neural-network/

4 *Telstra Corporation Limited v Phone Directories Company Australia Pty Ltd* (2010) 264 ALR 617

5 Ibid, 621.

AI in the arts

As a society, we have become increasingly comfortable with the idea that AI can be applied to produce non-creative outputs, such as data processing and analytics. We have even largely accepted the fact that, in some instances, AI can modulate or even replace the work of humans in particular industries. There has traditionally been resistance, however, to the notion that AI could parallel, or even come close to mimicking, the human imagination.

However, there are a number of examples that demonstrate the creative capabilities of AI.

For example, in 2018, *1 the Road* by Ross Goodwin became 'the first novel written by a machine'.[6] On the journey from New York to New Orleans, the AI machine consumed data generated from Goodwin's Cadillac car (which he had outfitted with a surveillance camera, GPS, microphone and clock) and produced a manuscript in real time. While 1 the Road is a strong example of the creative capabilities of AI, it was achieved with some very human elements of production, direction and independent intellectual effort. As noted by American critic Connor Goodwin, "[T]hough Goodwin has surrendered creative license to the writing machine, he nevertheless created the machine and the rules by which it operates".[7]

Paving the way for works like Goodwin's was a Japanese novel co-authored by an AI system in 2016, aptly titled *The Day A Computer Writes A Novel*, which passed the first round of screening in the Hoshi Shinichi Literary Award. The novel was generated by reassembling words and phrases deconstructed from a template novel authored by the human team working with the AI program. Although the team created a choice-matrix for the AI program to follow, the human input in the wording of the novel is arguably more evident than Goodwin's in *1 the Road*, as demonstrated by the novel's closing paragraph (translated by a report in The Japan News):

> *"I writhed with joy, which I experienced for the first time, and kept writing with excitement. The day a computer wrote a novel. The computer, placing priority on the pursuit of its own joy, stopped working for humans."*

The novel was entered in the prize two years after Hoshi Shinichi's daughter, Marina Hoshi Whytemade, allowed the inclusion of non-human authored entries. The fact that the judges were not told which works were authored by humans and which were not is an indication of the relative quality of the novel and the increasing maturity and flexibility of AI programs.

There are also a number of musical and artistic works which have been artificially created by non-human intelligence. For example, an AI machine developed by Facebook AI research, Rutgers University and the College of Charleston was able to generate artistic works after being trained on the characteristics of over 80,000 paintings from the 15th to the 21st centuries.[8] The AI software generated abstract art which rivalled human authors so much that some critics could not tell the difference.[9]

In the music world, American singer-songwriter Taryn Southern used machine learning in 2018 to create *I AM AI*, the first album to be entirely composed and produced using AI. Then there's 'Alice', AI developed by Australian start-up Popgun in 2017. Alice was initially skilled in listening to notes played by a human on piano and responding with an algorithm-based progression, however, 'she' went on to compose her own piano, bass and drums together as a backing track for human vocals.[10] Over the past year, Popgun have also been teaching an AI to sing.[11]

These examples are by no means exhaustive and as AI continues to advance in leaps and bounds the list will only grow. The 'computer-generated' works contemplated by the Australian Full Federal Court in *Telstra Corporation Limited v Phone Directories Company Pty Ltd* pale in comparison to today's technological applications. Indeed, to apply decade-old principles to the copyright issues arising from these developments is problematic to say the least.

6 Connor Goodwin, 'A.I. Storytelling: On Ross Goodwin's 1 the Road', Bomb Magazine, 14 December 2018, available at: https://bombmagazine.org/articles/ross-goodwins-1-the-road/

7 Ibid.

8 Elgammal et al (2017) 'CAN: Creative Adversarial Networks Generating "Art" by Learning About Styles and Deviating from Style Norms', paper presented at the International Conference on Computational Creativity (ICCC), Atlanta (20-22 June 2017), available at: https://arxiv.org/pdf/1706.07068.pdf

9 Igammal et al (2017) 'CAN: Creative Adversarial Networks Generating "Art" by Learning About Styles and Deviating from Style Norms', paper presented at the International Conference on Computational Creativity (ICCC), Atlanta (20-22 June 2017), available at: https://arxiv.org/pdf/1706.07068.pdf

10 Jacca-RouteNote, 'Is the future of pop music in artificial intelligence?', RouteNote, 6 November 2018, available at: http://routenote.com/blog/14880-2/

11 Popgun Labs, 'Popgun – Vocals', YouTube, 21 July 2019, available at: https://www.youtube.com/watch?v=cd4f4i3HQ4w&feature=youtu.be

Commercial implications: testing the IP 'rewards' system

The copyright system has been designed to protect and incentivise human intellectual effort. It does this by creating a framework in which, among other incentives, authors are rewarded financially for their work when it is used by others, and those who seek to circumvent this system are penalised. This framework is destabilised by the concept of AI authors – if AI-generated works are not protected by copyright because they have not been created by a human author then, theoretically, it follows that they could be freely exploited by anyone. This could have a chilling effect on investment in AI systems to produce creative outcomes.

One way for lawmakers to deal with this issue is to attribute authorship to the creator of the AI system. Indeed, other Commonwealth jurisdictions such as New Zealand and the United Kingdom have updated their copyright legislation to reflect the increasing role of technology and AI in creative works. In both these jurisdictions, the author of a literary, dramatic, musical or artistic work that is computer-generated is deemed to be 'the person by whom the arrangements necessary for the creation of the work are undertaken'[12]. This language is similar to the protections that exist under Australian law for creators of cinematograph films, being 'the person by whom the arrangements necessary for the making of the film were undertaken'.[13] However, it remains to be seen whether Australia will extend this concept of authorship to literary, dramatic and artistic works.

Even if Australia does move in this direction, there is a still a question of who the law would consider to be the person making the necessary arrangements for the work to be created – the maker or user of the AI program?

Some commentators have drawn attention to the complexities brought about by AI over other technological advancements. For example, "Microsoft developed the Word computer program but clearly does not own every piece of work produced using that software".[14] Rather, the copyright in those works is attributed to the user. However, the user's contribution in works generated through artificial intelligence is likely to be much less significant. For this reason, it would seem to make the most sense to attribute copyright ownership to the creator of the AI program. This would likely also have the flow on effect of stimulating the invention of, and investment in, creative AI systems.

In other jurisdictions, AI machines themselves have been given the status of creator. For example, music composing AI, Aiva (Artificial Intelligence Virtual Artist), recently became the first AI composer to be officially recognised by SACEM, the France and Luxembourg authors' rights society.[15] As a result, Aiva can now release music and earn royalties under its own name. This recognition signals a shift in attitudes towards the role of AI in the arts and helps to overcome problematic scenarios where computer-generated works are not protected against unauthorised use or reproduction simply because they do not have a human author. On the other hand, there may be some resistance to this idea, as the computer-generated author would not have expended the same emotional or intellectual effort / 'sweat of the brow' to produce the work, so why should users have to pay for it? The increasing role of AI in creative works creates further tension in the creator/user dichotomy.

Attributing authorship to the creators of AI systems may, however, be problematic from an infringement perspective. For example, if an AI system creates a work that is substantially similar to a pre-existing copyright work, will the creator of the AI system be responsible for that infringement? Is this an unintended consequence that goes to show just how much work legal systems have to do catch up to these technological advancements? This will surely be an area for further consideration in the near future.

12 *Copyright Act 1994* s 5(2); Copyright, Designs and Patents Act 1988 (UK) s 9(3).

13 *Copyright Act* 1968 (Cth) s 22(4).

14 Andres Guadamuz, 'Artificial intelligence and copyright', WIPO Magazine, October 2017, available at: https://www.wipo.int/wipo_magazine/en/2017/05/article_0003.html

15 AI Business, 'Aiva is the first AI to Officially be Recognised as a Composer', 10 March 2017, available at: https://aibusiness.com/aiva-is-the-first-ai-to-officially-be-recognised-as-a-composer/

What about moral rights?

A further consideration is how the law will deal with moral rights. Moral rights are distinct from economic rights under copyright law in that they attach to the individual author and cannot be assigned to another person, not even the copyright owner. These rights are an important element in the philosophical matrix of copyright law as they provide a sound legal acknowledgement of the integrity of the creative endeavour and help to further the objective to incentivise the creation of new works.[16] In this case, moral rights should theoretically attach to the individual human authors responsible for the creation of the AI system itself.

However, it will be interesting to see how this will play out in practice, particularly if and when these AI systems are used by people other than the creator. Will these users be required to attribute the creator each time they produce work via the AI system? What about instances where unsavoury creative works are produced using the AI system – will the creator's right against derogatory treatment be triggered? These are just some of the questions that come to mind.

Looking to the future: is Australia already behind?

Anxieties about the human authorship test in the Copyright Act are not new. In fact, over twenty years ago, the Australian Copyright Law Review Committee voiced concerns about the extent to which the Copyright Act in force at the time accommodated 'the increasing, indeed almost ubiquitous, use of computers in the creation of copyright subject matter'.[17]

As outlined above, there are already a number of economic and ideological considerations for Australian lawmakers to consider, and this list will only grow as AI technology advances.

Other common law jurisdictions around the world have already taken action to adapt to these advances, and Australian lawmakers will need to move quickly to ensure that Australian copyright law can cope with the many complexities brought about by the role of AI in content creation, particularly as we move into a post-pandemic world.

16 Australian Law Reform Commission (2013) Copyright and the Digital Economy, Report No. 122, 7.

17 CLRC, Parliament of Australia (1999) *Simplification of the Copyright Act 1968 — Part 2: Categorisation of Subject Matter and Exclusive Rights, and Other Issues*, 47–8 [5.10].

Contacts

James North
Head of Technology, Media and Telecommunications

+61 2 9210 6734
+61 405 223 691
james.north@corrs.com.au

Eddie Scuderi
Partner

+61 7 3228 9319
+61 419 731 560
eddie.scuderi@corrs.com.au

Adam Foreman
Partner

+61 2 9210 6827
+61 431 471 355
adam.foreman@corrs.com.au

Eugenia Kolivos
Partner

+61 2 9210 6316
+61 407 787 992
eugenia.kolivos@corrs.com.au

Alistair Newton
Partner

+61 3 9672 3483
+61 450 922 876
alistair.newton@corrs.com.au

Frances Wheelahan
Partner

+61 3 9672 3380
+61 419 517 506
frances.wheelahan@corrs.com.au

Arvind Dixit
Partner

+61 3 9672 3032
+61 438 278 463
arvind.dixit@corrs.com.au

Gaynor Tracey
Partner

+61 2 9210 6151
+61 423 859 363
gaynor.tracey@corrs.com.au

David Yates
Partner

+61 8 9460 1806
+61 414 465 928
david.yates@corrs.com.au

Grant Fisher
Partner

+61 3 9672 3465
+61 407 430 940
grant.fisher@corrs.com.au

Helen Clarke
Partner

+61 7 3228 9818
+61 411 399 643
helen.clarke@corrs.com.au

Michael do Rozario
Partner

+61 2 9210 6566
+61 416 263 102
michael.do.rozario@corrs.com.au

Jonathan Farrer
Partner

+61 3 9672 3383
+61 414 235 063
jonathan.farrer@corrs.com.au

Philip Catania
Partner

+61 3 9672 3333
+61 419 320 815
philip.catania@corrs.com.au

Jürgen Bebber
Partner

+61 3 9672 3260
+61 412 082 114
jurgen.bebber@corrs.com.au

Richard Leder
Partner

+61 3 9672 3489
+61 418 170 790
richard.leder@corrs.com.au

Justin Fox
Partner

+61 3 9672 3464
+61 417 220 275
justin.fox@corrs.com.au

Simon Johnson
Partner

+61 2 9210 6606
+61 412 556 462
simon.johnson@corrs.com.au

Kate Hay
Head of Intellectual Property

+61 3 9672 3155
+61 400 628 372
kate.hay@corrs.com.au

CORRS
CHAMBERS
WESTGARTH

This publication is introductory in nature. Its content is current at the date of publication. It does not constitute legal advice and should not be relied upon as such. You should always obtain legal advice based on your specific circumstances before taking any action relating to matters covered by this publication. Some information may have been obtained from external sources, and we cannot guarantee the accuracy or currency of any such information.

Sydney
Melbourne
Brisbane
Perth
Port Moresby

corrs.com.au