

TMT Technology, Media &
Telecommunications

The Australian Landscape 2019



WWW.CORRS.COM.AU

**CORRS
CHAMBERS
WESTGARTH**
lawyers



Technology, Media and Telecommunications

**Corrs Chambers Westgarth is Australia's
leading independent law firm.**

We provide exceptional legal services across the full spectrum of matters, including major transactions, projects and significant disputes, offering strategic advice on our clients' most challenging issues.

With more than 175 years of history and a talented team of over 1000 people, we pride ourselves on our client-focused approach and commitment to excellence. Our fundamental ambition is the success of our clients, and this is reflected in everything we do.

We advise on the most significant global matters and connect with the best lawyers internationally to provide our clients with the right team for every engagement. We are also at the forefront of some of the most high-profile public international law matters in our region, assisting governments and corporations with the resolution of highly complex cross-border disputes.

We are the firm of choice for many of the world's most significant organisations, with our people consistently recognised for providing outstanding client service and delivering exceptional results.

This publication has been prepared by the Corrs Telecommunications, Media and Technology team, one of the largest cross-disciplinary TMT teams in Australia with expertise spanning technology, corporate, intellectual property, regulatory, telecommunications and disputes. Technology issues are increasingly relevant to all sectors of the economy and we support clients across the lifecycle of a project from early stage venture capital investment, regulatory waivers to test new technology, shaping new regulatory regimes, and entrance into new markets through to tech and media transactions. We also advise on operational projects such as outsourcings, procurement, data governance and compliance. The Corrs TMT team is also recognised as having significant expertise in litigation and investigations across privacy, tech projects and high profile defamation suits. On the telecommunications front, we are known for our strength in complex and 'market first' projects including those relating to infrastructure rollout and sharing, spectrum, network security, regulatory, access arrangements, satellites and cable projects and mergers and acquisitions.

If you have any questions on the content of the publication, or about the TMT landscape in Australia, please let us know. Contact details for our team can be found on pages 12 and 13 of this publication.



James North
Partner and
Head of Technology,
Media & Telecommunications

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



Frances Wheelahan
Partner and
Editor of TMT: Australian
Landscape

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

Media

Defamation law reform – back on the agenda

Author: Richard Leder, Partner

It's been more than a decade since Australia unified its defamation laws nationally and introduced some key reforms (including a cap on general damages and a provision that excludes most corporations from being able to sue). Significant technological changes since that time, including the explosion of social media, have caused many to question whether the uniform laws are out of date.

Now, reform is on the agenda once again. In late February 2019 a discussion paper was released, *Review of Model Defamation Provisions*. The paper invites submissions on a series of questions, including:

- Should the right of corporations to sue for defamation be broadened or narrowed?
- Should there be a “single publication rule”, which could treat an initial hard copy publication and all subsequent repetitions on line as a single publication?
- Should there be changes to the circumstances in which juries can determine defamation cases?
- Should the truth defence be changed?
- Should the meaning of “reasonableness” in the qualified privilege defence be amended?

- Should the honest opinion defence change, particularly the question of who needs to hold what opinion when the opinions are being published digitally?
- Should a “serious harm” or other threshold test be introduced?
- Should the “innocent dissemination” defence be amended to better reflect the operation of ISPs, ICHs, social media, search engines and digital content aggregators?
- Should the cap on damages be changed, particularly in relation to aggravated damages?

The answers to some of these questions will seem obvious to readers in the USA, but it's important to remember that Australian defamation law does not operate any differently in relation to public figures than it does to others. Other questions will be familiar to readers in the UK, where aspects of defamation law now deal more effectively with issues raised by defamation through social media, in particular. The way in which the cap on damages operates has come into particular focus following Rebel Wilson's successful action against Bauer Media.

However those who remember the long road to reform in Australia in the 1990s and early 2000s might be forgiven for having some scepticism about where the reform process will go. Defamation laws are State

based and for any reform to take effect nationally, it requires each State as well as the Commonwealth to reach agreement. It's happened before, and can happen again, but much will depend on politics rather than sound decision making.

Digital Platforms Inquiry

Author: Arvind Dixit, Partner

Background: What is the Digital Platforms Inquiry?

In December 2017, the Australian Government announced a broad-reaching inquiry into the impact of digital platforms – i.e. search engines, social media and digital content aggregation platforms such as Google and Facebook – on competition in media and advertising services markets. The Digital Platforms Inquiry is investigating the effect of digital platforms on media content creators, advertisers and consumers, with a particular focus on consequences for the supply of news and journalistic content.

Preliminary report released – recommendations for significant reforms

The Australian Competition and Consumer Commission (ACCC) has now released its Preliminary Report, recommending a number of new regulatory structures and mechanisms aimed at addressing concerns about the market power of major digital platforms. If adopted, there will be significant ramifications (and an increased regulatory burden) not only for major digital platforms, but also potentially for smaller, specialised platforms, media businesses, advertisers and advertising intermediaries.

At a high level, the Preliminary Report recommends a number of amendments and measures aimed at:

- enhancing existing merger control to capture and better assess digital transactions;
- mitigating default bias by introducing browser and search engine setup choice screens;
- increasing the oversight and regulation of digital platforms, as well as reviewing the existing media regulatory regime;
- requiring greater assistance from digital platforms for a more effective removal of copyright infringing material;
- increasing consumer control over their personal information and strengthening privacy obligations; and
- prohibiting unfair contract terms and holding businesses to account for including unfair contract terms in contracts.

Proposed changes to privacy

The ACCC has proposed several changes to Australia's privacy framework that are intended to empower consumers to make informed decisions and have greater control over their personal information. These include:

- **GDPR-style obligations:** The ACCC is clearly drawing significant inspiration from the GDPR, with a number of recommended changes aligned to the GDPR. For example, the ACCC is considering whether "consent" be defined as "express" consent (rather than express or implied consent), as well as strengthening notification requirements around collection and use of personal information and introducing third party certification.
- **Opt-in consent for targeted advertising:** The ACCC is also considering "opt-in consent" for the use of personal information for targeted advertising purposes, specifically whether entities should be prohibited from collecting, using, or disclosing personal information of Australians for targeted advertising purposes without their express, opt-in consent. This requirement could have a major impact on the business models of digital platforms operating in Australia.
- **Direct right of action for individuals:** The ACCC has also recommended the introduction of a direct right for individuals to bring actions for breaches of their privacy, as well as a statutory cause of action for serious invasions of privacy. A key issue arising from this recommendation will be the ability to commence class actions for breach of privacy in Australia. Procedural controls associated with initiating class action claims are less onerous in Australia than in Europe, and generally speaking, means that class actions in Australia can be commenced more easily.

Technology



Consumer Data Right

Author: Philip Catania, Partner

Background – Australia's Consumer Data Right

The Commonwealth Government is implementing a new 'Consumer Data Right' (CDR) in Australia (on the back of a number of reports including a report on "Open Banking"). At a high level, the CDR regime will allow "consumers" to access certain data relating to them held by certain public and private data holders and require those data holders to transfer that data to accredited third parties for defined purposes.

The CDR regime will be primarily enacted through Australia's competition and consumer laws (with interaction with the existing privacy framework) and will impose a number of rights and obligations of participants under the CDR in any sector designated by the Commonwealth Government. The legislation is currently going through Parliament with a report to the Senate Committee due on 21 March 2019.

Who does the CDR apply to?

The Government will designate industry sectors to which the CDR will apply. Initially, the regime will be confined to the banking sector, first applying to Australia's largest banks (CBA, NAB, ANZ and Westpac), and will commence no later than 1 February 2020. The Government has announced that the energy

and telecommunications sectors will also be subject to the CDR regime, and it appears that the Government's intention is to eventually implement the CDR regime across all relevant sectors of the Australian economy.

Who can access the CDR?

'CDR consumers' will be able to access data under the CDR regime. Drafted broadly, CDR consumers are defined as a person to whom CDR data relates who is identifiable or reasonably identifiable from the CDR data. "Consumers" can be businesses including large corporates.

Key issues to consider

There are some potentially significant coverage and compliance issues including:

- **Broad range of data subject to CDR:** 'CDR data' includes certain classes of information designated as 'CDR data' for the relevant sector as well as any information derived from that designated data, as set out in the relevant designation instrument. This could capture a broad range of value-added data sets within an organisation, and appears to be intended to capture meta-data. This may need to be taken into account when data holders are developing innovative data applications.
- **Business information:** As possible CDR consumers, large business organisations may be able to obtain data about the use of a particular service from a

service provider and transfer that information to a competitive service provider. While there are 'privacy safeguards' in place, it is unclear how confidential and sensitive information will be dealt with.

- **Extra-territorial application:** The CDR applies not only to CDR data generated or collected in Australia, but also CDR data generated or collected outside Australia by or on behalf of a company registered under Australia's Corporations Act or an Australian citizen or permanent resident.
- **Contractual obligations:** As we've seen with the Australian Privacy Principles and most recently with the GDPR, we can expect to see organisations placing contractual obligations on their service providers to give effect to those organisation's obligations under the CDR, likely leading to another round of contractual amendments.
- **Privacy safeguards:** The CDR regime introduces a new set of principles called the Privacy Safeguards that need to be adhered to when it comes to CDR data. Organisations will need to be set up so that they can properly deal with the requirements of the Privacy Safeguards, which may necessitate (for example) keeping CDR data segregated from other business data.

Mandatory data breach notification in Australia: a year in review

Author: Helen Clarke, Partner

In a significant year for data privacy globally, the Notifiable Data Breach scheme in Australia commenced just over a year ago in February 2018. Overseen by Australia's privacy regulator, the Office of the Australian Information Commissioner (**OAIC**), the scheme was heralded as a privacy 'shake-up' to encourage better accountability amongst business and government in their handling of personal data.

The past year has highlighted some of the successes and challenges of the scheme, and some high profile data breaches have delivered a number of 'lessons learned'.

Data breaches notified: a snapshot

The OAIC received 812 data breach notifications from commencement of the scheme in February to the end of December 2018. This represents a huge increase from the 114 'voluntary' data breach notifications made to the OAIC in the 2017 financial year.

The OAIC quarterly reports with data breach statistics reveal some interesting trends:

- Almost 60% of the year's data breaches were caused by malicious or criminal activity, and just over 35% were caused by human error. This leaves only 5% caused by system error.

- The most prolific reporting industry is the healthcare industry, which alone represents over 20% of notifications for the year. It is followed by finance (including superannuation), and then legal, accounting and management services.

These statistics highlighting cyber security risk and human error as key factors also suggest that entities need to invest in technology and information security as well as in training their people and developing a 'privacy aware' culture.

Unfortunately, there is no indication as to whether these statistics include conservative notifications of data breaches that objectively may not meet the threshold of a 'serious' data breach. Nevertheless, the trends are indicative of trends in privacy weaknesses, and the industries most often being targeted (or otherwise suffering non-compliances).

Lessons learned: the PageUp data breach

There has been no high-profile regulatory enforcement action reported arising from the Notifiable Data Breach scheme.

The OAIC's most active involvement in regulating the scheme (other than reporting statistics) was in May/June 2018 when widely-used human resources software provider PageUp reported suspicious activity on its network.

If all you read was the joint announcement on the incident by the OAIC, the Australian Cyber Security Centre and IDcare, you could be forgiven for thinking that the incident was nothing major and handled in a role-model fashion by PageUp. The three organisations jointly assured the public that there was only evidence of data *access* by an unauthorised actor, with no evidence of *exfiltration* (taking a copy of the data). PageUp was applauded for regularly updating the public and its customers (which included a vast number of high profile Australian and overseas customers) about the incident.

However, if you look beyond the joint announcement, the PageUp incident demonstrates a difficulty when multiple entities are affected by a data breach and struggle to effectively allocate notification responsibility between them.

Under the scheme, if a data breach causes two or more entities to be deemed to have suffered a data breach (e.g. an IT provider's breach is also a privacy breach by the IT provider's customer), then only one entity need investigate and notify in accordance with the Privacy Act. Our experience is that too few entities have revisited their current services agreements to ensure that this division of responsibility is appropriately addressed.

This was demonstrated through the PageUp data breach, where PageUp decided it would not notify affected individuals, and information-poor PageUp customers had to decide whether to notify or risk non-compliance with the notification legislation. The result was a disparate array of data breach notifications from numerous organisations. For individuals who had applied for jobs with multiple affected PageUp customers, this meant receiving a number of notifications about the same incident.

The notifiable data breach scheme was designed to avoid the risk of 'notification fatigue', however it does not appear to have achieved this goal in the case of PageUp.

The year ahead

The OAIC's funding has not increased in line with the expansion of its statutory functions to notifiable data breaches, and it is reported to be struggling to stay on top of its workload. If this continues, the coming year (like last year) may also involve hundreds of notified data breaches but limited regulatory enforcement action for privacy non-compliances.

Nevertheless, even without enforcement action, the reputational impact of a data breach is potentially significant and organisations should continue to take information security risks seriously to avoid high profile media attention, which could erode consumer trust.

Australia's New Decryption Legislation

Author: Eugenia Kolivos, Partner

Despite widespread criticism from individuals and industry participants, Australia passed the controversial *Telecommunications and Other Amendments (Assistance and Access) Bill 2018* (Bill) on 6 December 2018. On 9 December 2018, the Bill received Royal Assent and became law in Australia.

Decrypting encrypted technologies

The most controversial aspect of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Act) is that it allows Australian law enforcement agencies to request or demand that "designated communications providers" provide assistance with the decryption of encrypted communications and data.

Designated communications provider

A "designated communications provider" is defined broadly, and could include most individuals and businesses in the communications supply chain.¹ Examples include,² businesses that operate messaging platforms such as WhatsApp, phone and internet service providers, technicians and retail repairers, developers of software used in connection with communication services and manufacturers of telecommunications equipment.

Exceptions to compliance

To balance privacy concerns and uncertainty as to whether it would be technically possible for providers to comply with a demand for assistance, the Act includes several exceptions to compliance.

The most significant exception prevents law enforcement from compelling a provider to implement a "*systemic weakness or vulnerability*". A "*systemic weakness or vulnerability*" is defined as something that affects a whole class of technology, as opposed to one or more specified technologies linked to an individual. The exception was designed to protect companies from having to build backdoors into their software or hardware which could compromise the security of all devices.

International implications

The Act is intended to impact foreign companies who provide relevant communications services with one or more end-users in Australia, as well as those companies that develop, supply or update software in connection with the service.

The laws include a defence for not complying with requested assistance if compliance in the foreign country would contravene a law of the foreign country. However, this defence does not cover situations where compliance in Australia could violate the laws of another country the provider operates in.³

Ongoing review

The Australian Parliamentary Joint Committee on Intelligence and Security (Committee) is conducting a review of the legislation, and so far has agreed on two amendments. This includes extending the “industry assistance” powers under the Act to government anti-corruption bodies.⁴ The Committee intends to release its final report on 3 April 2019.

Where to from here

With the Labor Party announcing that it will move amendments to the Act under the *Telecommunications and Other Legislation Amendment (Miscellaneous Amendments) Bill 2019* this year,⁵ it is important that foreign and local companies which may be classed as “designated communications providers” keep an eye on the legislation in 2019.

1 *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, sch 1, s 317.

2 Parliament of Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, Bills Digest No. 49 of 2018-19, 3 December 2018, 21.

3 *Ibid* 31.

4 Parliament of Australia, House of Representatives, Committees – Intelligence and Security Committee, Speech, Andrew Hastie MP, 12 February 2019.

5 Parliament of Australia, House of Representatives, Committees – Intelligence and Security Committee, Speech, Mark Dreyfus, MP, 12 February 2019.





Technology investment in Australia

Foreign investment in Australian technology: do we need a FIRRMA approach?

*Authors: James North, Partner
Justin Fox, Partner*

Recent changes to the way the United States regulates foreign investment in its technology assets have highlighted an interesting contrast to Australia's approach.

Late last year, President Trump signed into law the Foreign Investment Risk Review Modernisation Act (**FIRRMA**). FIRRMA significantly expands the type of transactions that are subject to review by the Committee on Foreign Investment in the United States (**CFIUS**), to include 'other investments' involving critical infrastructure, critical technologies or personal data.

Previously, CFIUS only had jurisdiction over those deals where the foreign investor acquired a controlling stake in the relevant technology owning company. The new approach gives CFIUS power to review deals that are structured in a different way, but which still have implications in terms of national security.

By way of an example, CFIUS can now review transactions which give a foreign party any form of

access to non-public technologies, representation on the board of the target or enhanced influence over decisions that go to the development of the technology, irrespective of whether the foreign investor acquires a controlling shareholding. It therefore picks up non-equity deals such as development funding agreements or licensing deals which may give rise to technology transfer risks.

This approach makes absolute sense in the context of technology assets, which are highly portable and difficult to protect once access has been obtained.

How does Australia's approach differ?

In contrast, Australia continues to regulate the acquisition of technology assets by foreign buyers through FIRB oversight under the Foreign Acquisitions and Takeovers Act (**FATA**). The FATA gives the Treasurer broad powers to intervene in a proposed acquisition of technology assets by a foreign buyer (or to impose conditions on the acquisition) where the proposed transaction would be contrary to the national interest.

FIRB has shown that it is willing to take a 'fit for purpose' approach to reviewing technology and data deals. By way of an example, we have seen FIRB negotiate bespoke access restrictions, operational conditions and governance controls as a condition to approving the acquisition of data centres or health service providers. In taking that bespoke approach,

FIRB has generally been able to strike a sensible balance between dealing with any national security concerns that arise from a particular proposal, and ensuring that foreign capital continues to be welcomed into the Australian technology sector.

However, FIRB can only apply that approach to those technology deals it actually has power to review. Many technology deals will fall below the monetary thresholds at which compulsory FIRB notification is required (generally \$266 million for privately owned acquirers). This is particularly true in the case of emerging technologies which have not yet realised their full value.

Moreover, FIRB's powers of intervention typically only arise where the foreign investor wishes to acquire more than 20% of the target's shares or will otherwise obtain enhanced influence over its corporate policies. This means that alternate investment structures, such as development agreements and licensing arrangements, will often not be reviewed.

The role of Australia's Critical Infrastructure Centre

The newly created Critical Infrastructure Centre (CIC) also plays a role. The CIC brings together various Government departments and intelligence agencies to manage national security risks arising from foreign involvement in Australia's critical infrastructure assets, including ports, electricity, water and gas utilities. The CIC also oversees security issues relating to Australia's telecommunications sector.

While the CIC doesn't have a specific role in regulating technology deals, it does advise FIRB on acquisitions involving technology companies which service critical infrastructure owners and operators. It also advises the Minister for Home Affairs on the use of the Minister's power under the Security of Critical Infrastructure Act 2018 to direct owners or operators of critical infrastructure assets to take or refrain from taking certain action. These powers are intended to be used as a last resort and only where significant issues of national security are at play. The fact that they exist, however, does give the Minister (and by extension the CIC) a platform from which to influence deal formation in the technology sector – at least where it touches critical infrastructure or telecommunications.

Looking ahead

The issue up for debate is whether FIRB and CIC have sufficient review powers to ensure that Australia's national interests are fully reflected in the way that technology deals are reviewed.

If Australia is to enjoy an end-to-end technology industry capable of monetising and commercialising innovation, FIRB will need to regulate the development

of emerging technologies that drive economic prosperity. This suggests that broader considerations beyond national security should be brought to account.

It is perhaps worth considering whether the FATA should adopt a sector-specific approach to technology and data deals, as is the case with foreign investment in the traditional media sector and agribusiness. Doing so would allow FIRB to review acquisitions of early stage technologies and take a 'longer lens' view of the industry.

While any changes would need to be carefully structured so as to not dissuade foreign investment, there may be a case for a FIRRMA approach.



New opportunities

Lift Off - Australia launches its National Space Agency

Author: Frances Wheelahan, Partner

Australia's space industry has been estimated to employ over 10,000 people and be worth AU\$3 - 4 billion. With the support of a newly established Australian Space Agency, the aim is to grow Australia's space industry to AU\$12 billion and create an additional 20,000 jobs by 2030.

Australia intends to capitalise on and promote its comparative advantages in relation to its geographical position and its reputation for research excellence and technical expertise in many areas that support the space industry supply chain.

The Australian Space Agency was established in July 2018 within the Department of Industry, Innovation and Science. The Space Agency will be located in Adelaide, South Australia. The Space Agency will provide a central point of contact for Australia's international and national engagement with the civil space sector. The Agency will provide a formalised structure to support, grow and transform the space industry in Australia and put space on the economic agenda as a national priority.

Australia's national science agency, the Commonwealth Scientific and Industrial Research Organisation (**CSIRO**), is also deeply invested in space technology and working with the Australian Space Agency as part of its [Future Science Platforms](#).

The Australian Space Agency has already established strategic industry partnerships with Airbus, Sitael Australia and Nova Systems as well as Memorandums of Understanding with international space agencies in France, the United Kingdom, Canada and the United Arab Emirates. In addition to these formal arrangements, Australian entities and government agencies collaborate with other international space agencies, including NASA, JAXA and DLR, providing for, among other things, access to data and data sharing.

So far the Australian Government has committed approximately AU\$260 million to develop positioning technologies and infrastructure that uses satellite data to detect physical changes, such as crop growth, water quality and soil and coastal erosion, in unrivalled detail.

With a mandate for significant sector growth, we expect to see further investment and opportunities for both national and international investment in this space in Australia.

Simplifying the funding process for Australian startups

Author: Jonathan Farrer, Partner

Australia's startup ecosystem has developed significantly over the past few years.

Launching a start-up is now relatively simple as the basic foundations for digital products and services are widely available (or can be outsourced) and are comparatively cheap compared to the dotcom era. Startups can utilise a range of grants and regulatory concessions, including tax incentives for investors and employees, and startup hubs and shared workspaces are now mainstream. Many universities and corporates have established accelerator programs. Technological developments such as cloud computing, open source software and application programming interfaces have also significantly reduced the cost of launching a company and bringing a product to market. Spurred on by these developments, many Australian entrepreneurs are launching new startups with disruptive or problem solving ideas and are seeking support and funding.

Despite the startup explosion, the process for raising startup capital in Australia has evolved slowly over the past few years and from our position, acting for both investors and startups, there is no clear or homogenised approach to either process or documentation. This can result in protracted negotiations, delays and deals falling over, meaning the cash injection that a startup needs may come too late or not at all.

Corrs has recently produced its Australian Startup Funding Survey, which highlights the lack of uniformity in Australian early stage capital raisings and some key differences between fundraising in the Australian market and other markets such as the United States.

Our survey found:

- a wide range of capital sources are used by Australian startups, with preference shares and convertible notes being the most common type of funding, but other sources of funding such as SAFE's, shareholder loans and other forms of capital are also sometimes utilised;
- many Australian startup companies do not have vesting regimes in place for founder shares, compared to the United States where vesting regimes are standard;
- tranches or milestones were used in almost half of the capital raisings in our sample, reflecting a more risk-averse approach taken by Australian startup investors than their global peers;

- the use of, and size of, employee options pools was generally lower than in the United States, reflecting the fact that many early-stage Australian startups have not yet secured professional management teams or a significant employee base, and perhaps that incentivising the team is not as fundamental to an investment; and
- there were different approaches taken by companies in areas such as special majority decision thresholds, drag and tag right thresholds, the use of restraints and exit provisions, reflecting the non-standardised approach in Australia.

With most participants in Australia's startup ecosystem sharing a common goal to simplify the startup funding process, a more united approach will hopefully soon make this a reality.

Online platforms (such as our CorrsEdge platform, which provides low-cost bespoke documents) can also play a role in reducing the cost and time to produce seed financing documents, while giving both investors and founders the comfort that they have fit-for-purpose documents that can continue to work as the business scales up.

Contacts



James North
Partner
**Head of Technology,
Media & Telecommunications**
Tel: +61 2 9210 6734
Mob: +61 405 223 691
james.north@corrs.com.au



Adam Forman
Partner
Tel: +61 2 9210 6827
Mob: +61 431 471 355
adam.foreman@corrs.com.au



Arvind Dixit
Partner
Tel: +61 3 9672 3032
Mob: +61 438 278 463
arvind.dixit@corrs.com.au



David Yates
Partner
Tel: +61 8 9460 1806
Mob: +61 414 465 928
david.yates@corrs.com.au



Eddie Scuderi
Partner
Tel: +61 7 3228 9319
Mob: +61 419 731 560
eddie.scuderi@corrs.com.au



Eugenia Kolivos
Partner
Tel: +61 2 9210 6316
Mob: +61 407 787 992
eugenia.kolivos@corrs.com.au



Frances Wheelahan
Partner
Tel: +61 3 9672 3380
Mob: +61 419 517 506
frances.wheelahan@corrs.com.au



Gaynor Tracey
Partner
Tel: +61 2 9210 6151
Mob: +61 423 859 363
gaynor.tracey@corrs.com.au



Grant Fisher
Partner
Tel: +61 3 9672 3465
Mob: +61 407 430 940
grant.fisher@corrs.com.au



Helen Clarke
Partner

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



Jonathan Farrer
Partner

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



Jürgen Bebbler
Partner

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



Justin Fox
Partner

Tel: +61 2 9210 3464
Mob: +61 417 220 275
justin.fox@corrs.com.au



Kate Hay
Partner

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



Michael do Rozario
Partner

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



Philip Catania
Partner

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



Simon Johnson
Partner

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

SYDNEY

8 Chifley
8-12 Chifley Square
Sydney NSW 2000
Tel +61 2 9210 6500
Fax +61 2 9210 6611

MELBOURNE

567 Collins Street
Melbourne VIC 3000
Tel +61 3 9672 3000
Fax +61 3 9672 3010

BRISBANE

ONE ONE ONE
Eagle Street
111 Eagle Street
Brisbane QLD 4000
Tel +61 7 3228 9333
Fax +61 7 3228 9444

PERTH

Brookfield Place Tower 2
123 St George's Terrace
Perth WA 6000
Tel +61 8 9460 1666
Fax +61 8 9460 1667

PORT MORESBY

Level 2, MRDC Haus
Port Moresby
National Capital District
111
Papua New Guinea
Tel +675 303 9800
Fax +675 321 3780

