EMERGING ISSUES

Australian Technology, Media and Telecommunications Industry 2022

Lawyers | McCullough Robertson

We are pleased to bring you the 2022 edition of the *Emerging Issues* for the Australian Technology, Media and Telecommunications (TMT) industry.

Emerging Issues highlights the legislative and policy developments which directly impact the future of the Australian TMT Industry, together with keeping you informed of future TMT news and trends.

We are also delighted to profile the core members of our extensive TMT team who, with the support of our full service firm, are available to provide support to you across your operations and investments. Please contact any of our team members for further information.

Finally, we hope you find this publication of value and we welcome any feedback you may have regarding its content.

Alex Hutchens
Head of Technology, Media and Telecommunications

Contents

Foreward

What a whirlwind year – it's hard to believe that we're already in November.

We began the year with a collective sense of hope that the worst of the pandemic might be behind us, but quickly moved into record floods in the Australian autumn, record fires in the Northern Hemisphere summer, and then found that COVID-19 case numbers were rising again, to the point where many organisations began shifting back to mandated working from home arrangements.

Amidst all of that, our Head of International, John Kettle, and I made it to the United States for a quick coast-to-coast trip, punctuated by a stop off at the International Association of Privacy Professionals (IAPP) Global Privacy Summit in Washington DC. It has been a couple of years since that particular conference was able to run, and the energy in the room was palpable.

High on the agenda there, and the regular topic of discussion from coast to coast, was the increasing regulation of privacy, technology and data. There is a lot of international regulatory activity, with new regulation in the United Kingdom and Europe, and ever-increasing enforcement proceedings around the world. Australia is no different.

We have our ongoing review into the national *Privacy Act 1988* (Cth) (**Privacy Act**), education and enforcement activity under the *Online Safety Act 2021* (Cth), the expansion of industries subject to the *Security of Critical Infrastructure Act 2018* (Cth), potential increases to penalties under a reform proposal to the Australian Consumer Law (which is increasingly used to enforce privacy-related issues) and very recent confirmation that the High Court will hear from Facebook on the territorial scope of the Privacy Act in connection with the Cambridge Analytica investigation.

To top it off, with the recent news of a number of data breaches involving large Australian companies, including Australia's second-largest telecommunications company, with the reported compromise of records relating to some 10 million customers. Both the Office of the Australian Information Commissioner and the Australian Communications and Media Authority have launched investigations focusing on the adequacy of the cyber security controls in place, and the necessity of the collection of the relevant records. This has sparked additional calls for increases to the penalties and enforcement powers already under review by the Attorney-General.

We will report on these cases in more detail in our 2023 TMT Emerging Issues, but it goes to show that the rate of change is as strong as it has ever been and we see this as continuing for 2023.

On the corporate side, McCullough Robertson's integrated corporate and tax team, led by 13 partners, has analysed its public and private deals over the last 18 months, focusing on the evolution of the commonly used "standard market clauses" such as 'bridging the price gap' and 'anti-embarrassment protection'.

Prepared specifically for in-house counsel and executives, we are pleased to share with you a practical summary of the key considerations that will impact your next transaction. Download the What's market for M&A here.

Finally, in this edition we explore important developments in employment law in light of the gig economy and consider whether crypto can be used to pay staff, intellectual property law in light of Artificial Intelligence and the metaverse and cyber insurance in light of ever-present cyber risks, amongst other things.

Alex Hutchens
Head of Technology, Media and Telecommunications

Contracting in the gig economy: the state of play in 2022 and beyond

While there are different ways that a worker can be engaged to perform work for a business, we've seen that independent contracting relationships have increasingly found favour with businesses operating in the 'gig economy' space.

As the nature of the tasks performed by workers in this space continue to evolve, the courts have been forced to grapple with disputes about the proper characterisation of gig workers' employment status, and, the duties and obligations that business operators and workers in the gig economy owe both to each other and third parties.

In two recent decisions, the High Court has refined the approach to determining whether workers are an employee or a contractor and, in doing so, emphasised the importance of the words of written contracts in what many commentators have fairly described as a "black letter" approach.

What's the difference, and why does it matter?

The fundamental difference between an employee and an independent contractor is the nature of the duties that they owe to a principal.

An independent contractor typically provides an agreed service under a contract, but does so in the course of carrying on an independent business or undertaking.

In contrast, an employment relationship is a contract for the provision of personal services to an employer by an employee, and is the subject of mutual common law and statutory obligations.

The correct classification of a worker as either an employee or independent contractor is important. Incorrectly classifying a worker can expose the principal to significant underpayment claims for wages, penalty and overtime rates, leave entitlements as well as penalties for sham contracting arrangements and breaches of other provisions of the *Fair Work Act 2009* (Cth) (**FW Act**). Penalties are not reserved for non-compliant businesses, but can also be imposed on an individual involved in a contravention of the FW Act.

Changes to the legal landscape

There is no clear test in legislation to determine whether a worker is a contractor or employee. The long-standing position at common law has been that it is necessary to consider the totality of the relationship between a putative employer and employee, which involves consideration of a broad range of factors, with no one factor being decisive.

This is known as the "multi-factorial test" which has been the subject of recent refinement by the High Court (discussed below).

An example of the kinds of factors typically considered when applying the multi-factorial test is set out below:

Factor	Characteristics of a 'typical' independent contractor	Characteristics of a 'typical' employee
Control	The worker exercises significant control over when, where and how they perform tasks.	The principal exercises significant control over when, where and how the worker performs tasks.
Ownership of tools and equipment	If substantial tools are required to perform tasks, the worker supplies and uses their own tools.	If substantial tools are required to perform tasks, the principal supplies tools to the worker for use.
Uniform	The worker wears the uniform of their own business, or no uniform at all.	The worker wears the uniform of the principal's business, or other clothing of their choice.
Method of payment	The worker issues invoices to the principal, and is paid on the basis of the services they issue invoices for.	The employee is paid at an agreed hourly rate for attendance at work, and may receive bonuses or commissions as agreed with the principal.
Business worked within	The worker works for their own business, and for the benefit of that business.	The worker works for the principal's business, and for the benefit of the principal's business.
Withholding of tax	Tax is not withheld from payments made by the principal. The worker collects and remits GST from payments made to them by the principal.	The principal withholds tax from payments made to the worker and remits tax to the Australian Tax Office.
Right to delegate	The worker is engaged to achieve a result and has a right to delegate the work required to achieve that result to others.	The employee enters a contract of personal service and must perform work personally without a right of delegation.

The High Court's recent guidance

In February 2022, the High Court published two decisions in which it considered whether workers were contractors or employees: *Construction, Forestry, Maritime, Mining and Energy Union v Personnel Contracting Pty Ltd* [2022] HCA 1 (**Personnel Contracting**) and *ZG Operations Australia Pty Ltd v Jamsek* [2022] HCA 2 (**Jamsek**).

In these decisions, the High Court emphasised that, where the parties have comprehensively committed the terms of their relationship to a written contract that neither party challenges the efficacy of, either on the basis that it is ineffective or otherwise a sham, it is not necessary or appropriate to determine the character of the relationship by a wide-ranging review of the parties' dealings, including post-contractual conduct.[1] Instead, the character of the relationship should be determined through analysis of all relevant contractual rights and obligations.

In practice, this means that it is critical for those who engage workers to ensure that their employees and contractors are engaged under written contracts and that the terms of those contracts clearly reflect the nature of the relationship intended by the parties.

Could an 'on-demand' workforce be covered by traditional (or new) modern awards?

Against the backdrop of the High Court's findings in *Personnel Contracting* and *Jamsek*, future developments in award coverage (and the potential development of new awards) are also possible.

In June 2021, we saw Menulog file an application under section 158 of the FW Act seeking the making of a new modern award to cover what it described as the *"on demand delivery services industry"* on the basis that existing modern awards that may apply to their workforce are not appropriate given that they do not recognise the on-demand nature of the business.

On 28 January 2022, the Full Bench of the Fair Work Commission concluded that the *Road Transport Award* covers employers and courier employees in this industry, but flagged future consideration of whether the coverage of the Award is consistent with its statutory objectives. If the Commission finds that it is not, it may determine that the *Road Transport Award* ought to be varied, or may even determine to create a new modern award altogether (as advocated for by Menulog).

If Menulog is successful, similar amendments or new modern awards could be developed for other industries, including TMT.

[1] *Personnel Contracting*, [59]; *Jamsek*, [48], [51].

Where to from here?

The High Court's decisions in *Personnel Contracting* and *Jamsek* underscore the difficulty of drawing a divide between these two distinct types of workers in the context of work arrangements – particularly where the common law test for drawing this distinction does not always easily accommodate digital platform-based working arrangements.

While these issues can be difficult to grapple with, there can be little doubt that the gig economy will continue to disrupt traditional business models and drive further technological innovation for years to come, and may soon begin to be accounted for in new or traditional industrial instruments.

As digital labour platforms continue to grow in scale and popularity and offer a widening range of services to consumers, getting the distinction between employment and contractor relationships right is critical to avoiding contravening civil remedy provisions in the FW Act, and to give certainty to the duties and obligations owed by each party to platform-based work relationships.

Scarlet Reid
Partner

Amber Sharp
Partner

Nathan Roberts
Special Counsel

Cyber Insurance in 2022 – market trends and key risks

It was only a short while ago that the debate about cyber insurance centred on how policies worked, whether they represented value for money and whether the risk of a cyber attack or event was 'real'. Many businesses remained in denial about those risks or they failed to address them adequately, through insurance and otherwise.

It turned out that the doomsayers were pretty close to being right about cyber risk being critical for businesses to deal with. The risks presented by cyber attacks are proving to be ever present, increasing it seems in both number and sophistication with each passing year. For example, the Australian Cyber Security Centre observes that there were some 67,500 reporting cyber crime reports in FY21, an increase of 13% over the previous year, at a cost of some $33 billion to the affected businesses.[2] This increase in number of incidents, and the significant financial impact of those incidents, has had a corresponding effect on the current state of the cyber insurance market.

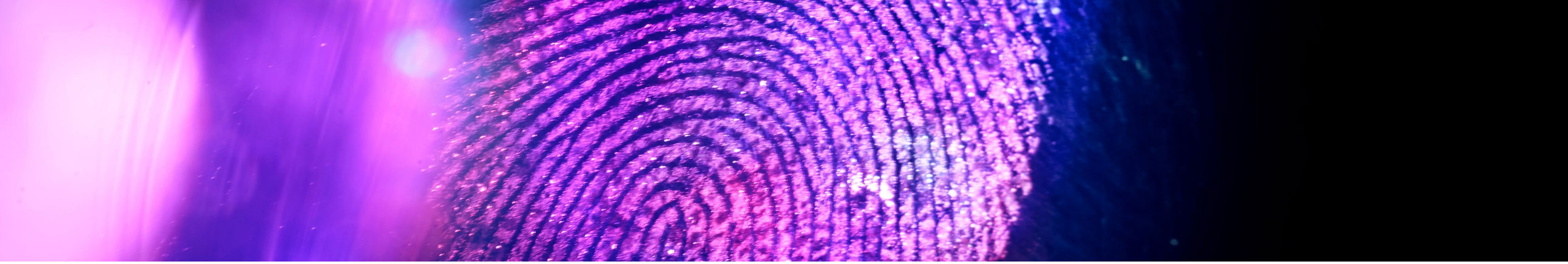
Market trends

Today, ransomware attacks stand head and shoulders above all other cyber risks including malware, social engineering and hacking by a factor of nearly three to one. Moreover, the **media, communications** and **technology sectors** are perceived by insurers as having the highest level of cyber risk, along with the **power and utilities** and **healthcare sectors**. According to IBM Security, these sectors have seen the average cost of cyber claims increase by between 20% and 70% from 2020 to 2021.

Ransomware attacks lead to two types of losses:

- the direct cost of dealing with the attack, ransom demand and releasing and restoring the system, and
- the corresponding loss of revenue or 'business interruption' while that process takes place.

[2] *ACSC Annual Cyber Threat Report - 1 July 2020 to 30 June 2021* available at https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21



For businesses that are themselves service providers on whom their customers rely, those losses can then extend to claims by those customers against the business for interruption to the customers' businesses and loss or compromise of their customers' data. Therefore, while attacks are becoming more frequent, the cost of each claim is also increasing due to the increasing dependence on continuous access to data and systems to run businesses, and the increasing amount and value of data stored in those online systems.

Insurers are responding to increased claim costs in the usual and predictable ways. They are adopting a greater level of scrutiny of new business and policy renewals, particularly for those insured clients who have had claims. They are looking very closely at the adoption of critical controls to prevent or minimise attacks and business continuity plans to ensure resilience.

Where adequate controls are not thought to exist or the overall risk level is assessed as being too high, they are either not providing cover or are reducing the levels of cover by imposing 'sub-limits'. In some cases, insurers have exited the cyber insurance market altogether, reducing competition and supply-side options. As a result of all these factors, those insurers who remain in the market are increasing premiums significantly, in some cases by more than 50%. The latter trend is predicted to continue in 2023, albeit not at quite the same levels.

The squeeze

Increasing insurance costs may be a familiar trend, but cutting costs by removing the insurance is not an advisable option. The regulatory scrutiny on cyber-security issues in Australia has never been higher than it is today. The mandatory notification of data breaches has been a feature of privacy legislation for some years now, but more broadly, the obligations and exposure are increasing as a result of:

- the introduction of additional obligations under the *Security of Critical Infrastructure Act 2018* in July for entities in the electricity, communications, data storage or processing, financial services and markets, water, health care and medical, higher education and research, food and grocery, transport, space technology, and defence industries;
- recognition of the potential for cyber security measures to form part of directors' duties, leading to potential personal liability on directors for failures to properly implement cyber security risk management practices; and
- a penalty of $60million for Google under consumer protection law for misleading statements about its data handling practices, demonstrating the risk under broader trade practices obligations.

Accordingly, it is more important than ever to consider cyber risks as a key business risk to be managed through a matrix of practical measures, contractual tools and appropriate insurance, properly tailored to provide the right level and type of cover.

Protecting your business – key risks to consider

For those businesses wanting to obtain and renew cover, they will need to work very closely with their brokers to present their risk in a way which is within the insurer's appetite to accept. The risks and considerations will be different for those businesses who are insuring their own losses only, those who operate in high risk sectors covered by critical infrastructure legislation and those who provide services to customers who will feel an impact from (and perhaps sue as a result of) any cyber security incident.

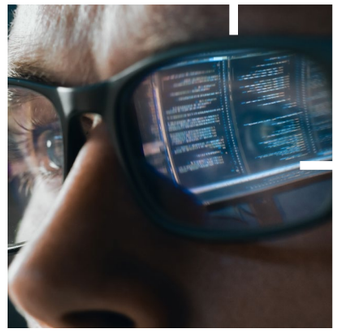
Detailed information will need to be presented about:

- the client risk profile,
- defence measures such as multi-factor authentication, endpoint protection software, endpoint detection and response,
- privilege access management and network security, and
- dedicated cyber business continuity plans, disaster recovery plans, incident response plans and functional and resilient backups.

The business will also need to have a keen sense of exactly what it wants to protect via its insurance program. Not all cyber risks are insurable and there needs to be a focus on the business 'crown jewels' when placing cover.

What we are seeing in the market at the moment is that without these measures and forethought, clients will struggle to secure and/or maintain cover. There is limited to no appetite from insurers for poorly managed risks.

As always, insurance remains just one of the means by which businesses will need to protect their IT assets and it remains equally important to have the necessary systems, policies, staff expertise and training to deal with that risk. In our previous article here, we outline the key elements to designing an effective cyber security framework and what cyber insurance can offer.



What's next?

We expect to see reductions in indemnity limits, as well as increases in premiums and policy deductibles, particularly in relation to ransomware claims. As mentioned, the heightened level of underwriting scrutiny of the insured risk is the other main trend likely to continue.

Businesses need to have a clear understanding of their cyber risk profiles and response plans and to ensure that they have cover with minimal gaps for key events. We recommend businesses undertake comprehensive Cyber Insurance policy checks to ensure cover is adequate, as well as a comprehensive cyber risk management plan in place.

Stephen White
Partner

Ian Dobbs
Executive Director, Allegiant IRS

Matt McMillan
Partner

Alex Hutchens
Partner

Trade mark infringement meets the metaverse

The metaverse – not to be confused with Marvel's multiverse – is an ambiguous concept which is continually morphing and expanding much like the cosmos itself. On a base level, the metaverse is an immersive online experience that exists by way of augmented or virtual reality technology and devices.

First coined by Neal Stephenson in his science fiction novel *Snow Crash* in 1992, the metaverse has taken off, as Big Tech and other industry players develop their own versions of the metaverse in their quest for total meta-market domination. The commercial opportunities are significant including by the exchange of blockchain-based assets such cryptocurrencies and non-fungible tokens (NFTs, that can be used as a certificate or proof of exchange of a particular version of a digital asset between a buyer and a seller) for virtual goods and services via online marketplaces for use in digital environments.

As brands increasingly embrace trading in virtual goods and services, the legal question has arisen: to what extent are existing trade mark registrations designating real-world goods or services enforceable in digital worlds by an action for registered trade mark infringement?

Registered trade mark infringement

In Australia, a person infringes a registered trade mark if the person uses "as a trade mark" a sign that is substantially identical with, or deceptively similar, to the registered trade mark in relation to the *same or closely related goods or services* for which the trade mark is registered. Although, the person is not taken to have infringed the trade mark if the person establishes that using the sign, as the person did, is not likely to deceive or cause confusion.

When considering infringement in the metaverse, it is import to consider:

- to what extent, if any, are digital goods and services traded exclusively in the metaverse considered to be the same or closely related to their real-world counterpart goods and services?
- to what extent, if any, are consumers likely to be deceived or confused as to the origin of virtual goods or services traded exclusively in the metaverse under the same or similar marks as their real-world counterpart goods and services?

Digital goods and services vs. real-world goods and services – what does this mean for brand owners?

The question of whether virtual goods and services occurring exclusively within the metaverse are the *same or closely related* to their equivalent real-world goods and services is yet to be tested by Australian courts.

Generally speaking, in determining whether goods or services are the same or closely related, consideration should be given to:

- the nature of the goods or services, their uses, and trade channels; and
- whether the goods or services would be acceptable substitutes or alternatives for the other.

While at first glance these factors may create a notable distinction between virtual and real-world goods and services; complexly, the metaverse is intended to mimic reality, and create an experience that spans both the digital and physical worlds. In these circumstances, there is a reasonable argument that virtual goods and services mimicking reality, and sold under the same or similar trade marks typically used in connection with their equivalent real-world goods and services, would be likely to deceive or cause confusion amongst consumers as to source, due to the perception of their digital equivalence in nature, use, and trade channels.

It is also worth noting that emerging Real-World Asset NFTs (**rNFTs**) experiment with "omniversal property rights" by bringing physical goods into the crypto economy. Essentially, rNFT is a method of using legal and software engineering to tokenise physical property such that it can be traded, collateralised, and owned in digital spaces.[3]

In circumstances where rNFTs grant the digital bearer the right to take physical custody of an equivalent underlying good, there is a credible argument that the distinctions between virtual and real-world goods and services will collapse in the mind of consumers, and that the use of the same or similar badge of origin in relation to both the digital and the physical manifestation of goods or services will be likely to deceive or cause confusion in trade.

United States trade mark infringement proceedings

In the United States, courts ask whether use of the defendant's trade mark, because of its similarity to the plaintiff's trade mark, is likely to confuse consumers. Under this test, trade mark registrations designating real-world goods and services are now forming the basis of complaints for trade mark infringement in the metaverse including:

- *Nike, Inc. v. StockX, LLC* – Nike, asserts its registered trade marks including for the SWOOSH Logo and NIKE (word) designating footwear (Class 25) and retail services (Classes 35 and 42) against online marketplace, StockX, for "minting" NFTs that prominently use Nike's trade marks, marketing those NFTs using Nike's goodwill, and selling those NFTs at heavily inflated prices to unsuspecting consumers who believe or are likely to believe that those "investible digital assets" are authorized by Nike when they are not (e.g.):

- *Hermès International v. Mason Rothschild* – French fashion maison, Hermès, asserts its registered trade marks BIRKIN (word) and BIRKIN trade dress designating handbags (Class 18) against artist, Mason Rothschild, for advertising, selling, and distributing METABIRKIN NFTs without Hermès permission and in violation of Hermès' trade mark rights (e.g.):

These proceedings are yet to be finalised as at the date of this article.

Where there's smoke, there's trade mark filings!

Trade mark filings around the world indicate brand owners from all industries are starting to prioritise seeking protection for new and existing trade marks in connection with the metaverse by designating virtual goods and services to new trade mark applications.

For example, in Australia:

- No. 2235833 Sushi Suhsiverse (SS IP Pty Ltd) – in connection with Class 9: non-fungible token (NFT) wallets and non-fungible tokens (NFTs);
- No. 2228876 PENFOLDS (Penfolds wine) – in connection with *inter alia* Class 9: digital materials, including crypto products, cryptocurrency, crypto tokens, non-fungible tokens, crypto collectibles, non-fungible assets, blockchain-based non-fungible assets and utility tokens; Class 35: operating online marketplaces featuring crypto collectibles and blockchain-based non-fungible assets; and Class 42: providing online virtual goods, namely, non-fungible tokens and;
- No. 2221389 (South Sydney Rabbitohs) – in connection with *inter alia* Class 9: virtual goods and digital media files authenticated by non-fungible tokens (NFTs); and Class 35: providing an online marketplace for buyers and sellers using blockchain and smart contracts for digital and crypto collectibles featuring players, games, records, statistics, information, photos, images, game footage, highlights and experiences in the field of rugby league.

For example, in the United States:

- No. 97251535 PANERAVERSE (Panera Bread) – in connection with *inter alia* Class 9: virtual food items and beverages for use in virtual worlds; Class 35: digital retail store services featuring virtual food items and beverages; and Class 41: providing on-line virtual restaurants and cafes in virtual environments;
- No. 97224598 NETAVERSE (Brooklyn Nets) – in connection with *inter alia* Class 41: broadcast of three-dimensional multi-camera virtual reality game services and; and
- No. 97212947 CROCS (Crocs) – in connection with *inter alia* Class 9: downloadable virtual goods created with blockchain-based software technology and smart contracts, in the nature of footwear; Class 25: online retail services featuring virtual goods, namely, footwear; and Class 41: entertainment and amusement, namely, provision of online non-downloadable virtual goods for use in virtual environments.

[3] https://medium.com/humanizing-the-sinsgularity/breaking-open-the-metaverse-with-real-world-asset-nfts-dccb00251fdf

If registered, the owners of the above trade marks will have robust protection in respect of their designated virtual goods and services in the metaverse, to the extent those marks can be enforced in their respective jurisdictions.

Filing strategies for the metaverse

Given the present uncertainties with enforcing trade mark registrations designating real-world goods and services in digital worlds, and the opportunistic behaviour of online traders in adopting famous third party trade marks in connection with their own virtual goods and services for sale in the metaverse; brand owners should consider actively pursuing a filing strategy to incorporate virtual goods and services, provided that is consistent with the use or good faith intended use of the trade mark.

If you are interested in knowing more about trade mark registrations and infringement in the metaverse, our Digital and Intellectual Property team can assist.

Belinda Breakspear
Partner

Harriet Young
Lawyer

Another one bites the DABUS – Full Federal Court allows appeal to hold that AI machine is not "inventor"

The definition of inventor in patent law has historically been held to bear its plain English meaning, being the natural person who invents, discovers, makes, or devises any new and useful process or product.

As artificial intelligence (**AI**) is increasingly capable of acts that would qualify a natural person to be an inventor, patent law globally is confronted with the question: whether an inventor may be other than a natural person?

This question has been considered in the recent decision of *Commissioner of Patents v Thaler* [2022] FCAFC 62.

Artificial intelligence: reinventing inventorship?

In 2019, the Artificial Inventor Project (**Project**) orchestrated patent applications around the world with the inventor named "DABUS, The invention was autonomously generated by an artificial intelligence".

The Project filed the patent applications with the intention of, among other things, providing industry guidance on patent laws relating to inventorship and AI-generated inventions.

In Australia, the Deputy Commissioner of Patents determined that the terms of the Patents Act and Regulations were inconsistent with artificial intelligence being treated as an inventor.[4]

On application for judicial review to the Federal Court of Australia, the primary judge took a different view, and found the Deputy Commissioner had erred in law by finding that DABUS could not be the inventor.[5] (For more background on the case, see our previous article: Australian appeal to determine future of global relationship with AI.)

The debate on whether AI can be considered an inventor under the Australian patent law now continues in the Full Court of the Federal Court of Australia, see Federal Court of Australia, Judgments.

[4] *Stephen L. Thaler* [2021] APO 5.
[5] *Thaler v Commissioner of Patents* [2021] FCA 879.

Australian law – human inventors only

In the recent Australian patent decision, the Full Court of the Federal Court of Australia (**FCAFC**) in *Commissioner of Patents v Thaler* [2022] FCAFC 62 has unanimously: [6]

- determined that a device characterised as an AI machine cannot be considered to be an "inventor" within the meaning ascribed to that term in the *Patents Act 1990* (Cth) (**Patents Act**) and the *Patents Regulations 1991* (Cth) (**Patents Regulations**); and
- allowed the appeal from the Commissioner of Patents from the decision of the Federal Court in *Thaler v Commissioner of Patents* (2021) FCA 879 on that basis.

Counsel for patent applicant, Dr Stephen Thaler, filed an application for special leave to appeal the decision of the FCAFC to the High Court of Australia (**HCA**) on 10 May 2022. The HCA has reportedly indicated it will hear oral arguments on the application for special leave in November 2022.

FCAFC decision

The Patent Regulations require a patent application to provide the name of the *inventor* of the *invention* to which an application relates (Regulation 3.2C(2)(aa)).

Section 15(1) of the Patents Act was therefore central to this appeal:

> Subject to this Act, *a patent for an invention may only be granted to a person who*:
>
> *a. is the inventor; or*
>
> *b. would, on the grant of a patent for the invention, be entitled to have the patent assigned to the person; or*
>
> *c. derives title to the invention from the inventor or a person mentioned in paragraph (b); or*
>
> *d. is the legal representative of a deceased person mentioned in paragraph (a), (b) or (c).*

The FCAFC disagreed with the primary judge that one may construe each of sections 15(1)(a), (b), (c), and (d) as alternatives, with the effect the latter three become their own sources of entitlement.[7]

The FCAFC found that:[8]

- the case law and the law relating to the entitlement of a person to the grant of a patent is premised upon an invention for the purposes of the Patent Act arising from the mind of a natural person or persons;
- where section 15(1)(a) provides that a patent for an invention may only be granted to "a person who is an inventor", the reference to "a person" emphasises, in context that this is a natural person; and
- therefore, on a natural reading of section 15(1), each of sections 15(1)(b), (c), and (d) provide for circumstances where a person becomes entitled to the grant of a patent by ultimately receiving that entitlement from the natural person(s) inventor in section 15(1)(a).

In other words, there must be a legal relationship between the natural person(s) inventor (section 15(1)(a)) and the person first entitled to the grant (sections 15(1)(b)-(d)); with the result that a device characterised as an artificial intelligence machine cannot be considered an "inventor" within the meaning ascribed to that term in the Patents Act and Regulations.[9]

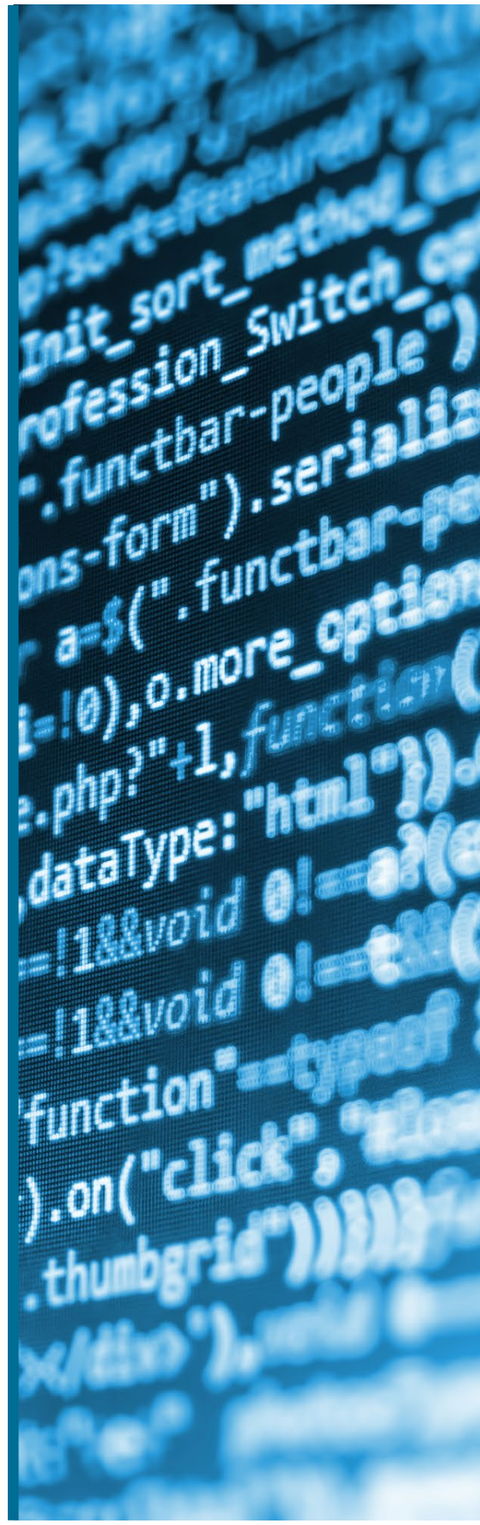
Practical takeaways

In practice, the holding of the FCAFC means that:

- only a natural person can be an "inventor" for the purposes of the Patent Act and Regulations in Australia; and
- such an inventor must be identified for any person to be entitled to a grant of a patent under sections 15(1)(b)-(d),

subject to successful appeal to the HCA.

However, the FCAFC observed that the characterisation of a natural person(s) as an inventor is a question of law; and the question of whether the subject patent application in dispute has a *human inventor* has not been explored and *remains undecided in this case*.[10] Had this been explored, it may have been necessary to consider what significance should be attributed to various matters including that: Dr Thaler is the owner of the copyright in the DABUS source code and the computer on which DABUS operates, and Dr Thaler is also responsible for the maintenance and running costs of DABUS.[11]



[6] At [1], [6], and [123].
[7] At [61], [112].
[8] At [105]-[107].
[9] At [107].
[10] At [121].
[11] Ibid.

What's next?

The FCAFC observed the development of patent law since 1624 has not until now been confronted with the question of whether an inventor may be other than a natural person.[12]

Debate on the role that AI may take within the scheme of the Patents Act and Regulations in Australia is important and worthwhile.[13] However, the Court must be cautious about approaching the task of statutory construction by reference to what it might regard as desirable policy, imputing that policy into legislation, and then characterising that as the purpose of the legislation.[14] In other words, we consider this is a matter for the legislature.

Notably, legislatures around the world are starting to engage in requests for comments on AI and inventorship, and AI and intellectual property generally. As AI increases in importance for intellectual property policy makers, the World Intellectual Property Office is also hosting conversations in this space, which may foreshadow an international treaty implicating AI inventions in the interest of harmonising intellectual property systems.

In the meantime, careful consideration should be had when filing patents in Australia, with due consideration being given to whether inventions devised by AI systems are capable of being attributed to a human inventor for filing purposes.

If you have questions about the issues discussed in this article, please get in touch with a member of our Digital and Intellectual Property team.

Belinda Breakspear
Partner

Alex Hutchens
Partner

Matt McMillan
Partner

Harriet Young
Lawyer

[12] At [115].
[13] At [119].
[14] At [120].

Unfair contract terms: subject of new civil penalties and other changes?

A review of the Unfair Contract Terms (**UCT**) regime by the Government in late 2018 revealed that while protections for small businesses in certain industry sectors had improved, it did not provide strong deterrence against businesses using UCT in their standard form contracts. On 27 October 2022, the *Treasury Laws Amendment (More Competition, Better Prices) Bill 2022* (**Bill**) was passed and awaits royal assent.

What you need to know

While the Bill is largely similar to the former Liberal government's *Treasury Laws Amendment (Enhancing Tax Integrity and Supporting Business Investment) Bill 2022*, it was re-introduced by the current Government with bi-partisan support. If passed, the Bill will amend the Australian Consumer Law under schedule 2 of the *Competition and Consumer Act 2010* (Cth) (**ACL**), as well as the *Australian Securities and Investments Commission Act 2001* (Cth) (**ASIC Act**), by continuing to strengthen the UCT regime.

The Bill, if passed without any significant changes, will:

- expand the class of contracts covered by the UCT provisions by providing new thresholds for what constitutes a 'small business contract';
- provide further clarification to the definition of a standard form contract by providing additional criteria for courts to consider; and
- introduce civil penalties for a breach of the UCT provisions, and establish two separate prohibitions which are breached if a person:
  - proposes an unfair term in a standard form consumer or small business contract; or
  - seeks to apply, or rely on, an unfair term in a standard form consumer or small business contract.

Key changes

Expanded class of contracts covered

Currently, the UCT regime applies to a 'small business contract' for the supply of goods or services, or a sale or grant of an interest in land, if one party to the contract is a business that employs fewer than 20 persons, and the upfront price payable under the contract does not exceed the applicable monetary thresholds.

The new Bill will apply the UCT provisions to an expanded class of contracts as follows:

- under the ACL, a small business contract will be covered if one party to the contract is a business that employs fewer than 100 persons or has a turnover for the last income year of less than $10,000,000; and
- under the ASIC Act, a small business contract will be covered if the upfront price payable does not exceed $5,000,000, and one party to the contract employs fewer than 100 persons or has a turnover for the last income year of less than $10,000,000.

Notably, the Bill removes the upfront contract value threshold for small business contracts under the ACL.

While the current UCT provisions state casual employees are not counted unless employed on a regular and systematic basis, the Bill provides part-time employees are to be counted in an appropriate pro rata fraction of their full-time equivalents.

Standard form contract definition

The Bill further clarifies what constitutes a 'standard form contract'.

In addition to the items a court must already consider when deciding if a contract is a standard form contract, the Bill provides that a court must also consider whether one of the parties has made another contract, in the same or substantially similar terms, prepared by that party, and, if so, how many such contracts that party has made.

The Bill also clarifies that a contract may still be a standard form contract even if a party:

- has had an opportunity to negotiate change if they are only minor or insubstantial in effect;
- is permitted to select a term from a range of options determined by the other party; or
- to another contract has been given an opportunity to negotiate the terms of that other contract.

Prohibitions and civil penalties

Currently, where a term in a standard form consumer or small business contract is found to be unfair, it will be void. However, the Bill is set to impose civil penalties for breaches of the prohibitions in the UCT regime in line with those under the ACL and ASIC Act.

In particular, if a person proposes, applies, relies or purports to apply or rely on, an unfair contract term, the maximum civil penalties available will be:

- for individuals – $2,500,000; and
- for corporations – the greater of:
  - $50,000,000;
  - three times the value of the benefit received; or
  - 30% of the adjusted turnover during the breach turnover period for the act omission.

A new 'breach turnover period' will afford a minimum period of 12 months for the penalty period from when a business contravenes the act to when it ceases to do so.

Expanded court powers

In addition to the new civil penalty provisions, the Bill provides a range of new powers to the court when dealing with UCTs. In particular, under the Bill, the court can make orders to:

- void, vary or refuse to enforce any part, or all of a contract to redress, in whole or in part, loss or damage that has been caused to any person as a result of the UCT, or to prevent or reduce loss or damage that is likely to be caused;
- make orders preventing a person from entering into future contracts that contain a term that is the same or similar in effect to a declared UCT; and
- prevent a person from applying or relying on a term in any existing contract that is similar in effect to a declared UCT regardless of whether the other contract is before the court or not.

Practical implications

The proposed changes, if passed, will have wide reaching implications for businesses by expanding the types of contracts captured. Businesses using standard form consumer or small business contracts should seek to conduct an audit of their existing contracts due for renewal, as well as review new or varied contracts prior to execution, to identify which, if any, terms may be caught by the new proposed UCT regime under the Bill.

A term will be unfair if:

- it would cause a significant imbalance in the parties' rights and obligations arising under the contract;
- it is not reasonably necessary to protect the legitimate interests of the party who would be advantaged by the term; and
- it would cause detriment (whether financial or otherwise) to a party if it were to be applied or relied on.

Terms that are likely to offend the UCT regime include:

- unilateral termination or variation rights;
- imbalanced indemnity clauses or limitations of liability;
- terms that penalise only one party for breach or termination of the contract; and
- automatic renewal clauses where a party is not given a prior opportunity to terminate the contract.

Importantly, the updated UCT regime will apply to all new contracts entered into after the commencement of the relevant changes, as well as any contract which is renewed or amended following commencement. Commencement is scheduled to be 12 months following the Bill being passed.

If you would like to discuss the practical implications of the Bill, or need assistance in conducting a UCT review of your standard form contracts, please get in touch with a member of our Digital and Intellectual Property team.

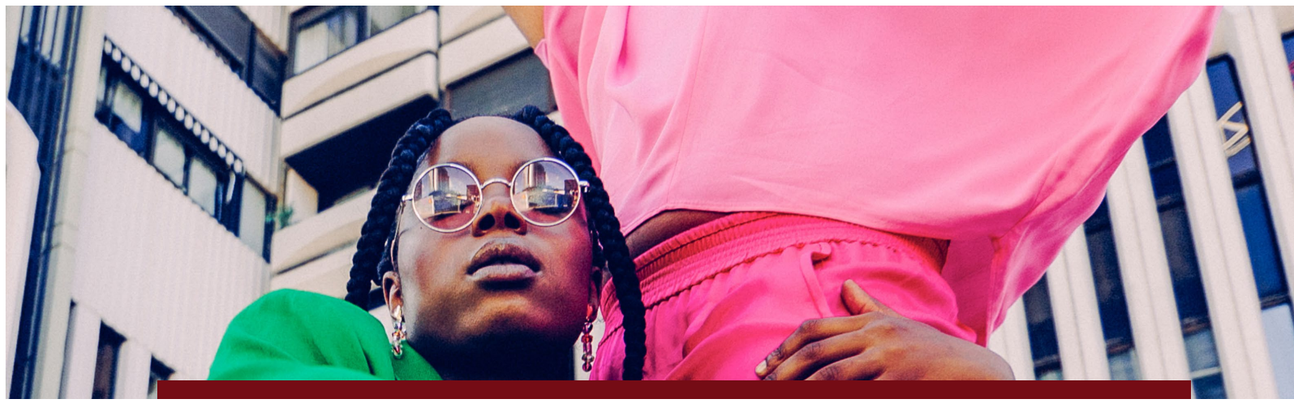
Alex Hutchens
Partner

Belinda Breakspear
Partner

Matt McMillan
Partner

Kirby Amos
Senior Associate

Watch this space



#watchout - New regulatory focus on influencers about

Brand ambassadors and social media influencers have been around for years, but the pandemic has provided the perfect environment for even further growth in the space. Celebrities and 'every day people' are increasingly using their social media platforms to promote third party products. So perhaps it's no surprise that a number of regulators have been paying particular attention to ensure that consumers are being appropriately protected. This is especially true in relation to financial services and also therapeutic goods which are currently under the microscope. Our article, Influencing for profit – the new Therapeutic Goods Advertising Code 2021 – what you need to know, addresses the changes in relation to therapeutic goods. In this article we focus on the implications when engaging influencers in relation to financial services (**finfluencers**).

Financial products – the rise and fall of 'Finfluencers'

*The Corporations Act 2001 (*Cth) (**the Act**) requires that a person must be authorised under an Australian Financial Services Licence (**AFSL**) to give financial product advice. A definition of providing financial product advice is broad – and applies if a finfluencer makes a recommendation or statement of opinion which is intended to influence another person's decision in relation to a financial product. However, many of the finfluencers we come across online – ranging from celebrities promoting crypto to that friend of yours who always has a great way to earn a 'passive income' – are not AFSL holders. To date, these finfluencers seem to have been flying under the radar – but that seems to have come to an end.

What's new?

In November 2021, Australian Securities and Investments Commission (**ASIC**) Commissioner, Cathie Armour, released an article 'Regulatory risk and finfluencer engagement for company directors' highlighting that companies should be mindful of the risks of engaging finfluencers. In the article, the Commissioner noted, in particular, that:

- a finfluencer generating income from content clicks or views may give rise to a conflict of interest or result in advice that's not in consumers' best interests. Even if the finfluencer was licensed, that would likely be a breach of law given the conflict of interest; and
- ASIC has noticed (and is monitoring for) market misconduct, such as "pump and dump" schemes where promoters buy shares in a company – then engage a finfluencer to "pump", the share price by creating a sense of excitement so the promoter can dump their shares at an inflated price.

In March 2022, ASIC published an information sheet (**INFO 269**) *Discussing financial products and services online guide* - this time aimed at the finfluencers themselves. INFO 269 reminds finfluencers that they are prohibited from carrying on a business of providing financial services without an AFSL – and that such a prohibition can be triggered if the influencer receives any kind of payment or benefit in return for making the statements.

Further, it specifically noted that a finfluencer promoting a unique link to access an AFSL holder's trading platform for which the influencer receives a pay-per-click could amount to dealing by arranging (also prohibited unless the finfluencer is, or is acting as the authorised representative of, an AFSL holder or benefits from another exemption). The guide also reminded finfluencers of their obligation not to engage in misleading or deceptive conduct in breach of Australian consumer law.

Since the release of INFO 269, there have been reports of a meeting between ASIC and about 30 popular finfluencers – with leaked audio recordings hinting that ASIC would be taking a harder line on the definition of 'financial advice' and also what it means to be 'dealing by arranging'.

What this means for financial services companies engaging finfluencers

The implications of being in ASIC's spotlight for finfluencers are fairly clear – they are now on notice that ASIC is watching this space and will take action if it is in the public interest. However, companies should also be mindful of the risks when engaging finfluencers in connection with their financial products and services. For example, a company whose financial products are promoted by a finfluencer could be liable under section 79 of the Act for aiding, abetting, counselling or procuring the breach of the Act. Companies may also be considered to have engaged in misleading and deceptive conduct in their own right, including if finfluencer content is posted or shared on their company social media pages.

There are severe penalties for breaches of the Act (including up to five years imprisonment for individuals and upwards of $1 million for corporations). Engaging in misleading and deceptive conduct in breach of Australian consumer law can also result in fines of the greater of $10,000,000; three times the value of the benefit received; or 10% of annual turnover of the company in preceding 12 months, if court cannot determine benefit obtained from the offence.

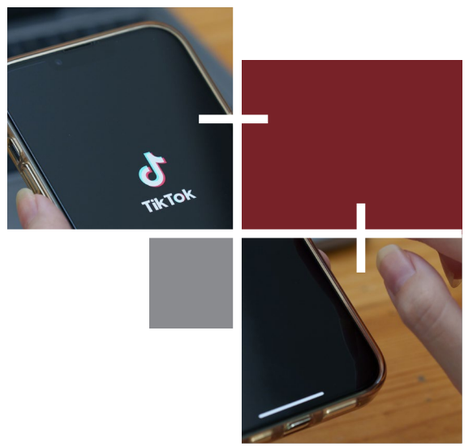
Accordingly, for AFSL holders engaging finfluencers, it will be important to:

- do due diligence - know who the finfluencer is, know their audience and also how they approach their content creation and publication. This also assists in ensuring compliance with design and distribution obligations;
- have appropriate risk management systems and monitoring processes - this should include guidelines which apply to the finfluencer in relation to content creation and publication, including steps to ensure that the finfluencer is not doing anything that gives rise to a conflict of interest, or could otherwise put you in breach of your AFSL conditions; and
- have sufficient compliance resourcing to monitor your finfluencers - this might include pre-approval rights, or rights to require content to be promptly removed on request – and also to ensure that you're meeting the design and distribution obligations relating to your AFSL.

Alex Hutchens
Partner

Rebecca Lindhout
Special Counsel

With special thanks to Eadie Melloy for her assistance in writing this article.



Paying employees in a growing crypto market

Given the growing cryptocurrency market, employers, particularly in the tech industry, have started asking more often: can we pay our workforce in cryptocurrency? Offering cryptocurrency as part of the salary package can attract tech savvy candidates and suggests a forward-thinking company culture. There are ways to pay employees in cryptocurrency, but there are complexities.

Can employers pay employees in cryptocurrency?

The Fair Work Act 2009 (Cth) (**FW Act)** governs the employment relationship in most Australian workplaces. Section 323 of the FW Act requires employers to pay wages and salary "in money" by one of a number of specific methods. Those methods are:

- cash;
- cheque, money order, postal order or similar order;
- electronic funds transfer; or
- another method authorised under a modern award or an enterprise agreement.

Money is not defined in the FW Act, however, when section 323 is read in the context of other legislation, such as the *Anti-Money Laundering Counter-Terrorism Financing Act 2006* (Cth), the *A New Tax System (Goods and Services Tax) Act 1999* (Cth) and the *Currency Act 1965* (Cth), cryptocurrencies should be understood as "digital currencies" rather than "money". Consistent with that view, the Australian Taxation Office (**ATO**) issued Taxation Determination TD 2014/25 which concluded that cryptocurrency does not satisfy the meaning of money. That determination said (at paragraph 24):

> *It has been argued that bitcoin satisfies the ordinary meaning of money because on a functional approach it satisfies three essential elements for money because it serves as (1) a medium of exchange, (2) a unit of account, and (3) a store of value. In addition, it is argued that there is widespread usage and acceptance of bitcoin in the community as a means of discharging debts and making other payments, and accordingly bitcoin's increasing acceptance has now reached the point that it qualifies as 'money'. This later point is very much a question of fact and degree. The evidence available to the Commissioner informs the view that the current levels of use and acceptance of bitcoin within the community is far short of what may be regarded as sufficient or necessary to satisfy the test in Moss, nor is it a generally accepted medium of exchange as per Travelex.[29] Accordingly, bitcoin does not satisfy the ordinary meaning of money.*

Accordingly, the default position is that wages or salary owed to employees cannot be paid in cryptocurrency. However, there are still ways to incentivise employees with cryptocurrency.

Other options to pay employees in cryptocurrency

While employers must generally pay amounts payable to employees in money, an employer is permitted to deduct an amount payable to an employee in the limited circumstances set out in section 324 of the FW Act. Those circumstances include where "the deduction is authorised in writing by the employee and is principally for the employee's benefit", such as a salary sacrifice arrangement under which the employee chooses to forego an amount payable to the employee in relation to the performance of work and, instead, receive some other form of benefit of remuneration such as cryptocurrency.

However, there are taxation implications of doing so. The ATO has said that where an employee has a valid salary sacrifice arrangement with their employer to receive cryptocurrency as remuneration instead of Australian dollars, the payment of the cryptocurrency is a fringe benefit (similar to paying an employee's gym membership or allowing an employee to use a work car for private purposes). As such, the employer will be subject to the provisions of the *Fringe Benefits Tax Assessment Act* 1986 (Cth) and fringe benefits tax (**FBT**) which is payable by the employer at the rate of 47% (although it may be reduced by post-tax contribution by the employee).

The relatively high FBT rate may make this an unappealing option for many employees given that it may impact the overall value of an employee's salary (depending on their arrangements with their employer). There are also FBT reporting obligations imposed on an employer.

Alternatively, rather than paying an employee cryptocurrency on a pre-tax basis under a valid salary sacrifice arrangement, an employer could agree to facilitate the conversion of a portion of post-tax remuneration into cryptocurrency after it has been paid as money. This could be done by establishing a third-party account into which money is paid (on behalf of the employee) and then converted into cryptocurrency. If this option is to be pursued, employers and employees should ensure that there is an agreement with respect to any transaction costs and risk allocation with respect to fluctuations in the value of cryptocurrency – in particular, ensuring that any tax payable upon the conversion or dealing in cryptocurrency (a capital gains tax asset for tax purposes) will rest with the employee.

Can contractors be paid in cryptocurrency?

In the growing gig economy, individuals are frequently engaged as independent contractors to perform freelance work, rather than employed as employees. The payment of contractors is not subject to the FW Act and its restrictions on the form of payment. In theory at least, contractors may, like any corporate entity, agree to be paid in any medium of exchange such as shares, options or cryptocurrency.

However, the taxation implications remain complicated. The ATO has provided limited guidance in this regard, only noting that parties who provide services may be rewarded with tokens whose money value is "ordinary income of the recipient at the time the tokens are derived". While this may assist contractors with better understanding their reporting obligations, businesses should seek specific tax advice when paying contractors in cryptocurrency given the complex tax treatment of cryptocurrencies.

Where to from here?

We've seen an increase in the number of employers, particularly Tech companies, seeking to find ways to incentivise employees through cryptocurrency. The FW Act does not currently permit employee's ordinary wages and salary to be paid in cryptocurrency. However, cryptocurrency can be paid under a valid salary sacrifice arrangement as well as companies who provide payroll services whereby an employee's wages or salary are paid in money into an account (in accordance with the FW Act) and that money is then converted into cryptocurrency.

With the recent decline in the value of major cryptocurrencies, cryptocurrency interest has begun to dissipate. However, we expect employers to continue to seek ways to incentivise staff through means other than traditional cash. Needless to say, any related employment contract which offers income by non-traditional means will require careful drafting.


Melinda Peters
Partner


Nathan Roberts
Special Counsel


Michaela Garcia
Lawyer

Meet the team

Operating for over 96 years, McCullough Robertson is an independent, Australian law firm with a proven track record of providing a range of legal services to the Technology, Media and Telecommunications industry. Known for our focus on operational excellence, we leverage our commercial and industry expertise to strategically support our clients from inception, during expansion and into maturity. Our teams work seamlessly together to deliver an unrivalled whole of project service, tailored to your industry.

For further information, please contact one of our team members:

Digital and Intellectual Property

Belinda Breakspear
Partner and Co-Head of Media
+61 7 3233 8968
bbreakspear@mccullough.com.au

Alex Hutchens
Partner and Head of Technology, Media and Telecommunications
+61 2 8241 5609
ahutchens@mccullough.com.au

Matthew McMillan
Partner
+61 2 8241 5644
mmcmillan@mccullough.com.au

Rebecca Lindhout
Special Counsel and Co-Head of Media
+61 2 8241 5683
rlindhout@mccullough.com.au

Corporate Advisory and Tax

John Kettle
Partner and Head of International
+61 7 3233 8962
jkettle@mccullough.com.au

Melinda Peters
Partner
+61 7 3233 8675
mpeters@mccullough.com.au

Reece Walker
Partner and Head of Life Sciences
+61 7 3233 8654
rwalker@mccullough.com.au

Ben Wood
Partner and Head of Start-ups
+61 7 3233 8913
bwood@mccullough.com.au

Litigation and Dispute Resolution

Tim Case
Partner
+61 7 3233 8960
tcase@mccullough.com.au

Peter Stokes
Partner
+61 7 3233 8714
pstokes@mccullough.com.au

Insurance and Corporate Risk

Stephen White
Partner
+61 7 3233 8785
stephenwhite@mccullough.com.au

James Lynagh
Special Counsel
+61 7 3233 8906
jlynagh@mccullough.com.au

Employment, Work health and Safety

Amber Sharp
Partner
+61 2 8241 5608
asharp@mccullough.com.au

Nathan Roberts
Special Counsel
+61 2 8241 5694
nroberts@mccullough.com.au

Visit our website for client results and expertise **www.mccullough.com.au**

Lawyers | McCullough Robertson

McCullough Robertson

As a fiercely independent Australian-grown law firm, we deliver more than outcomes. We strive towards a diverse and inclusive environment that supports our values and creates a collaborative and innovative experience for our people, our clients, and our community partners.

www.mccullough.com.au

BRISBANE | SYDNEY | CANBERRA | MELBOURNE | NEWCASTLE