Lawyers | McCullough Robertson

Emerging Issues

Australian Technology, Media and Telecommunications Sector Insights

July 2020

Welcome

We are pleased to bring you the July 2020 edition of *Emerging Issues* for the Technology, Media and Telecommunications (**TMT**) sector.

We had a great response to our previous edition, and while the rate of change in the TMT sector is always swift, it does feel that amongst all of the issues around COVID-19 the pace in the intervening months has been particularly relentless. Not only have we seen rapid organisational change across the public and private sector as workplaces pivot to large-scale remote working, but also constant developments with potential vaccines and treatments, intense regulatory interest in Australia, United States (**US**) and the European Union (**EU**) in the activities of large tech platforms – including a congressional inquiry in the US and new proceedings in Australia against Google – and the landmark Schrems II decision, to name just a few.

To that end, we're introducing a new section in this edition which covers breaking news in a shorter format to keep you up to date with evolving issues which we expect will involve multiple updates over time.

Of course, we also continue with our more in-depth coverage of topical issues. In this Emerging Issue, we take an in-depth look at: the implications of the recent Data Protection Commission v Facebook Ireland Limited (C-311/18) decision and what it means for Australian businesses sharing data globally; developments in defamation law in the context of a number of recent Australian decisions regarding the liability of online media platforms; current opportunities and challenges facing the adoption of blockchain technology, particularly smart contracts; and what the digital shift in Australian clinical trials means for the life sciences industry.

In our short form section, we cover the recent Twitter data breach, pending media reforms in Australia, the rise of investment apps and the competition regulator's proceedings against Google. We will continue to provide further developments on these updates in future editions – watch this space!

Our team of industry experts can advise you across all aspects of your operations, from new product development to managing a remote workforce. If you would like further information on any of the updates provided in this publication, please contact one of our team members on page 28.

We hope you and your families continue to stay safe and well in these unprecedented times, and hope you enjoy this edition.

Alex Hutchens
Head of Technology, media and telecommunications

Publish date: July 2020

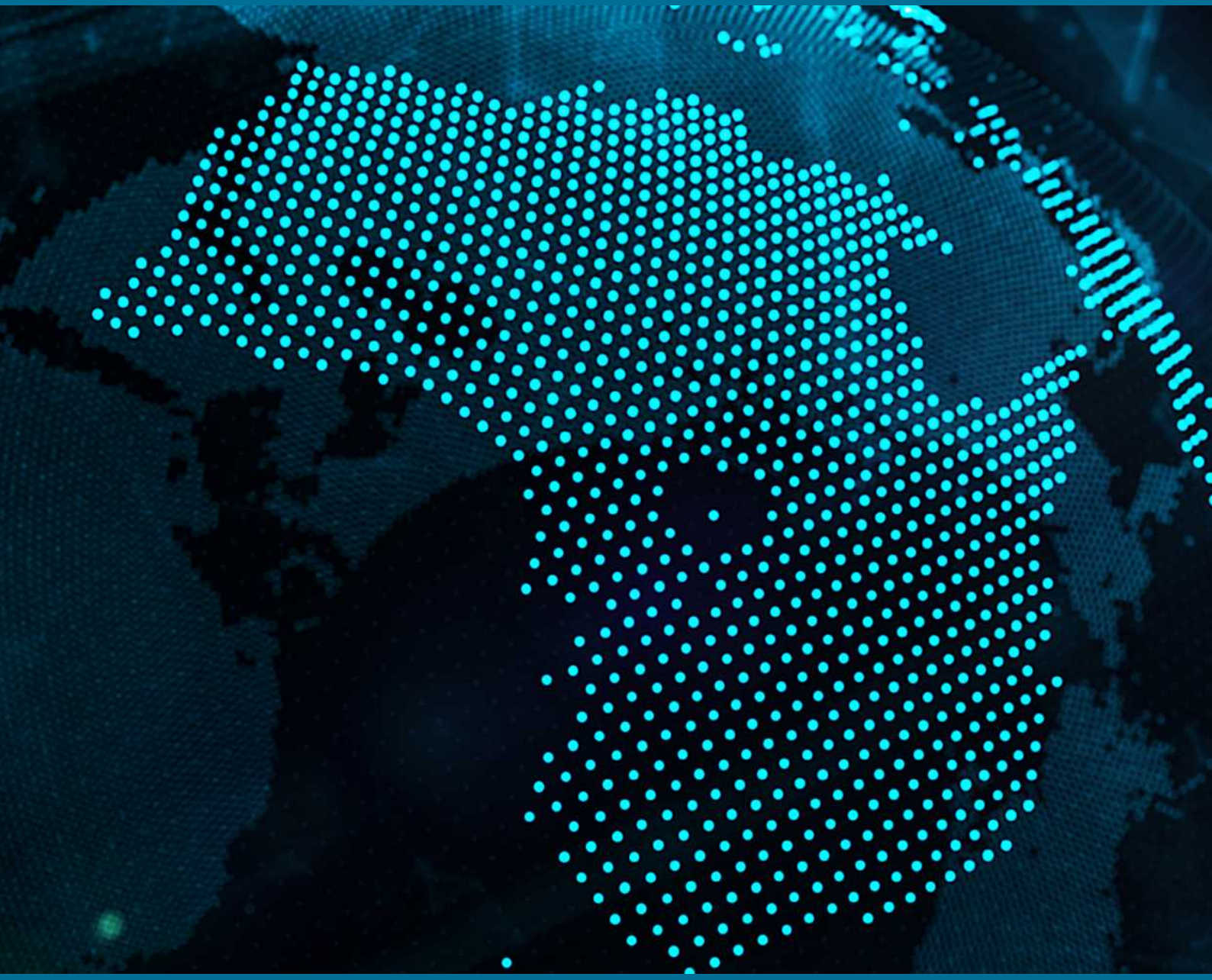

16t GVM
AND OVER
LEFT TURN
FOLLOW
40

Contents

Receive the latest industry news and updates to your inbox

Stay up to date by subscribing to our mailing lists and receive the latest news for the TMT industry in Australia.

Not sure if you have signed up? Visit our website to sign up or update your contact details and preferences. http://bit.ly/McRsubscribe



Schrems II - A view from downunder

INTRODUCTION – THE CHALLENGE OF EXTRA-TERRITORIALITY FOR NON-EU BUSINESSES AND GDPR

Since the introduction of the General Data Protection Regulation (**GDPR**) in 2018, Australian businesses, like other non-European Union (**EU**) domiciled businesses around the world, have grappled with the extra-territorial operation of the GDPR, particularly in the absence of a body of clear judicial interpretation on the point. It led to something of a compliance conundrum for businesses without an EU establishment but who were arguably targeting individuals in the EU in the ordinary course. Local EU Member State regulatory guidance provided some indicia by which to assess this issue, but was only just that, guidance, as to whether GDPR applies.

The potential for significant penalties for non-compliance with GDPR only exacerbates an approach by Australian businesses in their capacity as controller (where they are aware of this and of the need to make a conscious

self-assessment where they have no EU establishment) which has tended to the conservative insofar as GDPR compliance is concerned. This has given rise to significant cost in the absence of that clear judicial interpretation.

Of course, where the Australian businesses act in the capacity of processor for a controller who has an EU establishment (or is otherwise caught by GDPR and is aware that it is caught), the application of the GDPR is a given, and controllers flow through the standard contractual clauses (**SCCs**) as part of their data processing agreements (**DPAs**) with the processor.

The pace of international commerce, and the need for data flows to support global business models – the oil of the 21st century as we commonly hear – demand immediate compliance. In many cases, these data flows relied on the Privacy Shield (for United States-based transfers), and the SCCs (for both US and non-US transfers). Consequently, this has led to GDPR becoming a ubiquitous data protection standard given the need of most businesses engaged in international trade to engage with the EU, so that what is an internal European standard has rapidly morphed into a quasi-global one. With that reach has come uncertainty and that uncertainty is reinforced by this recent decision.

The decision on 16 July of Court of Justice of the European Union (**CJEU**) in case C311-18 (**Schrems II**) presents significant issues for parties involved in such data flows. Of course, much of the interest in the decision focuses on its invalidation of the US-EU Privacy Shield. This is entirely understandable given it was relied upon by so many parties to ensure the lawfulness of data transfers to the US from the EU. So whilst Australian businesses are largely unaffected by that (save where they are using US processors in relation to the EU-originated data and who themselves rely on the Privacy Shield), they are significantly impacted by the discussion of the appropriate use of SCCs.

Schrems II raises significant practical questions about the use of SCCs to effect lawful transfers of data from the EU to countries without adequacy decisions. This has potentially huge implications for businesses based in Australia receiving EU data, and even more complex implications for Australian businesses who receive EU data but also have operations or infrastructure in other non-EU jurisdictions, especially in respect of those jurisdictions which would not satisfy the requirements for an adequacy decision or on analysis of equivalence.

The CJEU's decision is instructive (rather than welcome) to the extent it offers judicial interpretation about the validity of the Privacy Shield and SCCs but its implications give rise to such uncertainty for granular compliance that it may ultimately be the catalyst that drives a hastening of regulatory alignment around the world. In casting doubt on the sustainability of business models that involve data flows to countries without adequacy decisions, prompting uncertainty for global data flows and leading to significant work for data exporters, data importers and the supervisory authorities in charge of those parties all over the world, it inexorably will demand a response wider than merely from within the EU itself. This is the unintended consequence of such informal extra-territoriality in a digital world.

THE BACKGROUND AND THE DECISION

As a brief recap, the Schrems cases relate to a complaint filed with the Irish Data Protection Commissioner in 2015 by Austrian Max Schrems, which challenged the legal basis for Facebook's transfers of data from Ireland to the United States of America (**USA**).

The CJEU in the first Schrems case (C-362/14) struck down the US-EU Safe Harbour Framework (the predecessor to Privacy Shield). However, it was subsequently revealed that Facebook had in fact relied on the SCCs to transfer the data to the US, not the Safe Harbour.

Accordingly, Schrems amended his complaint to challenge the SCCs themselves (and any other basis for data export). While he did not complain about the Privacy Shield arrangement itself, the CJEU felt it necessary to provide an opinion on that mechanism. As it turns out, that was a monumental decision.

In its Schrems II decision, the CJEU made several significant findings. In summary:

- the GDPR applies to transfers of personal data for commercial purposes from a party in the EU to a party established in a third country, even if that data may be subject to processing by the government in the recipient country for public security, defence, and State security;

- the level of protection provided by the SCCs must be read in the context of the legal framework of the recipient country, including regarding any access to data by public authorities in the recipient country, and the legal rights of the data subject in that country;

- supervisory authorities are required to suspend or prohibit transfers to countries where the protection for the data does not provide equivalent protection to that in the EU;

- the SCCs are valid (but subject to the overarching adequacy of the data protection arrangements including as a result of applicable laws in the recipient country); and

- the Privacy Shield is invalid, because certain US laws which allow US Government access to data, and the absence of appropriate data subject remedies, means there is not the same level of protection as there is in the EU.

IMPLICATIONS FOR AUSTRALIAN PARTIES (AND OTHER DATA RECIPIENTS WITHOUT ADEQUACY DECISIONS)

For Australian parties used to dealing with questions of extra-territoriality, there is another key area of inquiry to focus on.

It is uncontroversial that any transfer of data from the EU must be made in accordance with Articles 45 and 46 of the GDPR. Australia does not have adequacy recognition under the GDPR, and so in order for data to be transferred lawfully out of the EU to Australia, those transfers must effectively be made in accordance with either the SCCs or binding corporate rules (we acknowledge there are limited other possibilities – like contractual necessity – but they are not relevant for the purpose of this discussion).

Given that most entities do not have approved binding corporate rules, the most commonplace approach is through the use of SCCs. While the decision did confirm that SCCs can be a valid basis for transfer out of the EU, it also confirmed that this is only the case if two additional conditions are satisfied:

- the data exporter and the recipient of the data must take proactive steps to verify, prior to any transfer, whether there is an 'adequate' level of protection in the recipient jurisdiction; and

- the recipient must inform the data exporter of any inability to comply with the SCCs, and the exporter must in that case suspend the transfer of data and/or to terminate the contract with the recipient where there are no additional safeguards in place to adequately protect the data to the standard required by the GDPR.

Further, it is clear that where a controller does not suspend or cancel the transfer, competent supervisory authorities are required as part of their duties to step in and suspend or prohibit a transfer of personal data to the recipient country where they take the view that the SCCs are not being, or cannot be, complied with in that country, and that the protection of the data transferred that is required by EU law cannot be ensured by other means.

These conditions provide significant practical challenges for the parties and the supervisory authorities.

As to the first point, it is unclear in practice how a comprehensive assessment can be made. The concern with the Privacy Shield that ultimately led to its being invalidated was the fact that the US surveillance regime overrode the SCCs (because US government surveillance could happen irrespective of the SCCs being signed), the US surveillance program itself failed the proportionality principle (because it involved the indiscriminate collection of data), and data subjects did not have adequate enforcement rights, so the CJEU was not satisfied that the US law provided an adequate level of protection. For similar reasons, the use of SCCs to support transfers to the US would appear to present difficulties.

Given the tests for adequacy set out in Article 45(2) of the GDPR, there is a significant burden in having to make that assessment. Even for a party with the willingness and means to perform that assessment, it is no easy task. A party needs to assess the legal regime in the recipient country to determine whether there are rights of access to data for Government that are inconsistent with the GDPR, and to determine whether data subjects have equivalent enforcement rights as under the GDPR.

Without even beginning to start that assessment, it appears to us that there are real questions to be answered here in the context of Australia's regime. Australia itself is part of the 5-eyes intelligence community (together with the USA, United Kingdom (**UK**), Canada and New Zealand) which gathers and shares intelligence material, no small part of which is gathered through various forms of surveillance. There are numerous laws in Australia governing surveillance and data access, which in the main relate back to public safety and national security. It is not immediately obvious what level of national security surveillance is acceptable without offending GDPR standards, and so clearly there are some similarities between the Australian and US regulatory landscapes which require further consideration. Separately, data subject rights under Australia's *Privacy Act 1988* (Cth) do not fully align with the data subject rights under the GDPR. Clearly, there would be concerns too about the transfer of

data to countries like China and business or service models which facilitate such.

These dynamics, together with the complexity of understanding all surveillance powers and conducting complex equivalence assessments, raise a real question as to whether Australia's data protection landscape, as with many other non-EU jurisdictions, present effectively equivalent protection, or is actually a similarly flawed regime to that of the US.

As to the second point, the requirement is onerous. Not only does it impose an ongoing monitoring burden on the recipient, but it requires the exporter to have immediate contingency plans so that it can comply with its own obligation to suspend the transfer or cancel the contract (or react if a competent supervisory authority steps in). Whether this is realistic in the real world is doubtful. More likely, it makes the transfer of data to parties outside the EU a less attractive commercial option.

Finally, supervisory authorities themselves are required to be proactive in assessing and monitoring the circumstances of overseas data transfers (and presumably, the changes in those overseas laws that might subsequently make compliance with the standard contractual clauses impossible). Given the multiplicity of authorities, how they make these assessments, and whether there is coordination between them remains to be seen. Will an informal list of 'adequate' jurisdictions evolve; will there be a spate of adequacy applications?

SO, WHO SHOULD BE MOST CONCERNED?

The CJEU has highlighted that the onus is on businesses and national data protection authorities to scrutinise transfers, and the parties' ability to comply with the SCCs, on a case-by-case basis. Therefore, anyone who is a party to the SCCs ought to be reviewing their data flows, data handling practices and be analysing their ability to comply with the additional conditions. This was, admittedly, already part of the SCC regime, but we would hazard a guess that it was not uniformly complied with and many will find this focus on the additional assessment requirements to be a new challenge.

Based on what we see in data transfer arrangements, a few common scenarios spring to mind for Australian parties as being particularly high-risk.

- **The Australian processor:** Australian processors that provide services to EU-based controllers will face additional scrutiny and questions about the Australian regime and their data handling practices. They may see a reduction in demand for services, or a reduction in data transfers, or perhaps a detailed discussion around what other bases of transfer may exist outside the SCCs.

- **The Australian controller with an EU establishment:** Australian controllers with European presences who engage processors in countries without adequacy, will need to conduct the adequacy analysis and be prepared to be able to suspend or cancel transfers where the level of protection is not sufficient.

- **Australian processors and controllers who themselves use US vendors:** The use of US-based cloud services that provide storage, computing and analytics on demand through the cloud is commonplace. Many, but not all, of the large players have publicly confirmed in the wake of the decision that they intend to keep using SCCs. Depending on the nature of services used, the jurisdiction selected (including whether a fixed location has been specified), and the data flows, both controllers and processors may find that the Privacy Shield invalidity and ongoing questions about SCCs mean that further inquiries need to be made into the sustainability of these arrangements.

- **The Australian multi-national corporate group:** Possibly most complex of all, any Australian corporate group which relies on SCCs to export data from its EU entities to its Australian (or other non-EU domiciled) entities, will be affected. We see this as being potentially the most complex, because there is a likelihood for complex corporate groups that there are activities and infrastructure not only in Australia but also in other countries around the world. This is where the sheer enormity of the post-Schrems II task becomes apparent, because it may be that more than one countries' adequacy needs to be considered.

For a multinational group, it is more crucial than ever to understand its data flows, bases for processing, and supporting business practices. It is also fundamentally important to understand the broader legal landscape that may operate to undermine the literal meaning of the SCCs.

There are so many issues to address. To the extent data is being transferred to Australia, does the Australian legal landscape provide adequate protection? If not, are there other measures that can be taken to address that shortcoming? To the extent data handling (including through subprocessors) involves other jurisdictions, then the same questions arise in connection with those jurisdictions' laws.

Do you have infrastructure overseas, or do you engage sub-processors in other jurisdictions which do not have adequacy? If you do, what are those legal regimes like and do they have deficiencies that need to be addressed? Can they be?

It is foreseeable that it might be necessary to stop sharing data with certain countries altogether if the deficiencies in local laws cannot be overcome, and this may require data handling practices to be restructured. While the GDPR speaks to an analysis of the laws in the recipient country, we wonder if broader multi-jurisdictional considerations become relevant for multinational groups. For instance, in extreme cases, even if data is not transferred to a given country, particularly expansive overseas laws may seek to allow government access to data held outside a particular jurisdiction if an entity or group has operations or infrastructure in that jurisdiction. Could this mean that Australian operations become subject to overseas government access rights as a result of non-Australian operations, and would this be an issue relevant for the assessment of the adequacy of protections in Australia for that corporate group? That would provide another layer of complexity to the analysis and undermine data sharing practices and also potentially other aspects of corporate structuring.

It is clear that data sovereignty and national security and intelligence laws will be under the microscope, with potentially huge consequences for global data transfers. Those with complex data transfer regimes and operations in multiple jurisdictions will require prodigious knowledge of – or extensive advice around – the equivalence of international data handling laws.

SHOULD THE AUSTRALIAN FEDERAL GOVERNMENT BE CONCERNED AND SHOULD IT DO ANYTHING?

Given the potential impact on business and relationships, yes. However, the Australian Federal Government is in the process of negotiating free trade agreements with both the EU and UK right now and should seek to clarify the position of Australian data interests in these free trade agreements so that Australian public and private interests are not impaired by Schrems II.

FINAL THOUGHTS

This is not the first Schrems decision to disrupt global data sharing practices. After all, the first Schrems decision invalidated the Safe Harbour regime between the US and the EU. There was a grace period allowed for parties who had relied on Safe Harbour to adjust to the impact of the decision. It is unclear whether the same grace will be afforded to parties who relied on the Privacy Shield, although it is hard to see how there is any other option.

Quite apart from that issue, of greater importance for Australian parties is determining how to resolve the practical uncertainties that arise from the conditions required to support the lawful use of the SCCs. There is parallel work in the EU on the SCCs, and no doubt as a result of Schrems II there will be a flurry of activity amongst all interested parties.

The free flow of data is fundamental to modern commerce, and so we are confident that interests are aligned in ensuring a practical outcome. There is a clear role for global data regulators – not just competent supervisory authorities, although especially them - to coordinate on this point, and quickly, to provide some certainty on all sides as to what jurisdictions may be workable for data exporters and data importers alike. It also tends to suggest that in the interests of protecting domestic commerce, non-EU data protection regulators like Australia's Office of the Australian Information Commissioner should seriously consider working to obtain adequacy (including, as that will invariably require, amendments to local laws).

So this will be an evolving landscape in the short to medium term as the world digests the impacts of the decision. In the meantime, parties relying on SCCs must get to work on ensuring adequacy of protective measures as a whole, beyond merely the contract terms, and as ever from down under, data handling practices will appear for some to have been tipped upside down and significant uncertainty will exist in connection with EU-related data transfers.

Author
Alex Hutchens
Partner - Digital and Intellectual Property

Author
John Kettle
Partner - Corporate Advisory

Author
Rebecca Lindhout
Special Counsel - Digital and Intellectual Property

New year, new defamation scene: Australia's defamation laws set for a digital makeover in late 2020

AUSTRALIA'S DEFAMATION LAW SPACE IS ONE TO WATCH

In the latter half of 2020:

- pending the next *Voller*[1] appeal decision, news media providers will find out if they will continue to be liable for defamatory third party comments on their social media pages (and the scope of any potential defences);
- the ultimate outcome of *Kabbabe*[2] may see American social media conglomerates (Google, Instagram, Facebook) forced to divulge personal information about keyboard warriors who have used digital platforms to defame others;
- Geoffrey Rush's history-making defamation damages payment this June may contribute to capped damages reforms in upcoming federal defamation law overhaul; and
- after extensive public consultation, the Defamation Working Party's law reforms (led by New South Wales) were announced on 27 July 2020 and each state and territory is now expected to take steps to swiftly enact the *Model Defamation Amendment Provisions 2020* as part of the first phase of reform.

Despite this traction, Australia is still only on the precipice of a defamation law 'digital makeover'. Until seminal cases have exhausted their appeals, and reforms are introduced and tested, uncertainty lingers about *who* is liable for *what* kind of defamatory statements and just *how* much could defamation cost you?

FOOTNOTES: 1. Fairfax Media Publications; Nationwide News Pty Ltd; Australian News Channel Pty Ltd v Voller [2020] NSWCA 102.| 2. Kabbabe v Google LLC [2020] FCA 126.

As such, during this state of limbo, media industry stakeholders – news media houses, social media platforms, Australian businesses using digital platforms to promote their company and its offerings and those prone to making risky comments on the web – should take steps to help protect against defaming people under the law as it currently stands, as well as giving consideration as to how defamation law may look by the end of 2020 (and the impact that the changes to the Model Defamation Provisions will have).

LIABILITY FOR THIRD PARTY COMMENTS ON YOUR SOCIAL MEDIA PAGES – THE *VOLLER* SAGA CONTINUES

The latest New South Wales Court of Appeal decision in *Voller* confirms news media platforms are, broadly, 'publishers' of third party defamatory comments on their social media pages for the purposes of the *Defamation Act 2005* (NSW). While this satisfies a crucial element of defamation, another appeal is yet to determine whether defences are available to protect against liability for the defamatory slander by third parties in such circumstances. If defences are ultimately dismissed, the floodgates for defamation liability may open, and not just to news media companies, but any person or business that runs a public social media page which allows user generated content (including comments) to be shared.

Key takeaways: If you run a business in 2020, it is likely you also run active social media pages across a number of digital platforms. While removing these social media pages, making them private or disabling public comments will decrease risks of defamation claims, these options can be highly uncommercial for business – particularly in light of changing consumer engagement models as a result of COVID-19. Our practical suggestions for alternative ways to address the risk include:

- ensuring your business has internal social media policies and procedures for your business development, marketing social media teams. These policies and procedures should include:
    - a clear moderation policy, including how often content should be reviewed, and information about any filters which have been automatically applied, or should be manually applied by reviewers. These filters could include key words or phrases which are high risk;
    - guidance for identifying other defamatory (or potentially defamatory) material;
    - steps to be taken when that material is identified – whether that means immediate removal, or escalation to a member of the legal team for prompt further investigation. If material is to be removed, the policy should also provide guidance to ensure your team are only removing the affected comments (as opposed to negative comments about your business, for example, which, if removed, can amount to misleading or deceptive conduct under Australian consumer law);
- keeping the moderation policies refreshed. For example, if defamatory material which is identified relates to a 'hot topic', consider whether additional filters / key words should be added to your moderation policy (either temporarily or on a longer-term basis). This will ensure that your moderation policy remains as easy to implement as possible; and
- providing regular training (including refresher training and training for new team members) to ensure that the application of the policy is clearly understood, and consistently applied.

For more information about defamation in the social media context, including the types of statements found to cause a defamatory imputation, parties who are publishers, and the scope of damages, see the *Defamation: the Social Media, Social-distancing Edition* article written by Special Counsel, Rebecca Lindhout.

THE ANONYMITY OF KEYBOARD WARRIORS MAY SOON COME TO AN END

The ultimate outcome of the recent *Kabbabe v Google LLC* case may disrupt Australia's defamation laws, and consequently the anonymity of keyboard warriors, in big ways.

In that case, an anonymous person left an arguably defamatory Google review about Dr Matthew Kabbabe's Melbourne dental practice on Google. Kabbabe asked Google to remove the review. Google refused. Kabbabe then asked Google to provide information about the reviewer. Google refused again, arguing it did not have any means to investigate where and when the reviewer's ID was created. Consequently, Kabbabe sought leave from the Federal Court of Australia to file an originating application on Google in the United States compelling Google to disclose details about the reviewer so that Kabbabe may bring defamation proceedings against them. The Federal Court granted Kabbabe leave to serve the discovery request on Google.

This decision is insightful for a number of reasons:

- firstly, because Google was incorporated in America, and America is a signatory to the *Hague Service Convention*, the Federal Court allowed the service. This is important because the majority of digital platform and social media giants have their headquarters incorporated in America. It follows that Australian courts may grant leave for applicants to request discovery from, for example, Facebook and Instagram about people behind anonymous accounts or fake accounts who make defamatory comments; and

- secondly, the Federal Court considered it had jurisdiction to grant leave for the application because, by virtue of the review being left on the internet, it was accessible to each state and territory within Australia.

Key takeaways: If the *Kabbabe* case ultimately results in successful defamation proceedings, those leaving anonymous reviews online may need to critically moderate their comments on others' Google accounts or social media pages. Helpfully, people who consider they have been defamed through comments on digital platforms may now have a course of action to compel American digital platforms to take down defamatory reviews. For the online platforms, however, the decision is unlikely to be looked on favourably given the time and resources which they would be required to devote to dealing with such requests for information, and the impact it may have on the way individuals (and companies) use their platforms.

For more information about the *Kabbabe* case, please see our recent article *Anonymous reviewer cannot hide behind international borders*.

DEFAMATION LAW REFORMS ARE FINALLY HERE (OR AT LEAST NEAR)

The particular developments in defamation law canvassed above come in the context of a number of recent Australian decisions regarding the liability of online media platforms – particularly Google – for defamatory material available on their platforms.[3] While developments in that area are still in progress (it is hoped there will be a further working paper by the end of the year), there is some positive news on the reform-front.

After extensive public consultation, the Model Defamation Law Working Party has released long-awaited reforms to the existing Model Defamation Provisions. These reforms, the first in the defamation space since 2005, could restrike the balance between an individual's reputation and the right of a free and fair press, and generally bring Australia's defamation laws into the digital age. They include:

- the introduction of a 'single publication rule' which will dramatically reduce news media entities' exposure to defamation claims for archived stories. Currently, the limitation period for defamation proceedings resets every time a defamatory statement is 'published' – which currently occurs *every time* a reader views or downloads a news story online. This essentially results in an unlimited period during which defamation claims can commence in respect of such content. Instead, the limitation period will commence at the first publication (for online works, the time the work is uploaded);

- the introduction of a 'serious harm' threshold. This threshold will need to be satisfied as early as soon as practicable in the proceedings before the trial to filter-out insignificant claims at an early stage. This amendment will mean the defence of 'triviality' is no longer required, as the burden of proof relating to the seriousness of the harm will shift to the plaintiff;

- requiring the aggrieved person to issue a 'concerns notice' to the publisher of the material before defamation proceedings are commenced. In addition to these notices becoming mandatory, the information to be included will be more detailed to better allow a publisher to assess the merits of the claim at an early stage. The publisher can offer to make amends, which (if reasonable and compliant with certain requirements) may impact the defences available to the publisher or the ability of the aggrieved person to commence proceedings. The intention is to provide an opportunity for the publisher to make amends and 'right the wrong' in the hope of avoiding proceedings altogether or ending them as early as possible during proceedings (even once a trial has commenced);

- greater clarity on the damages for non-economic loss, with values to be expressed in ranges based on seriousness, rather than caps on liability; and

- a new defence to provide better protection for publication which is a matter of public interest, similar to the current United Kingdom model. When announcing the reforms, New South Wales Attorney-General Mark Speakman noted that the new defence is intended to restore '*balance to ensure reputations are protected while responsible speech is as free as it needs to be to shine lights into the dark corners of our society*'.

FOOTNOTES: 3. For example, Defteros v Google LLC [2020] VSC 219.

FINAL THOUGHTS

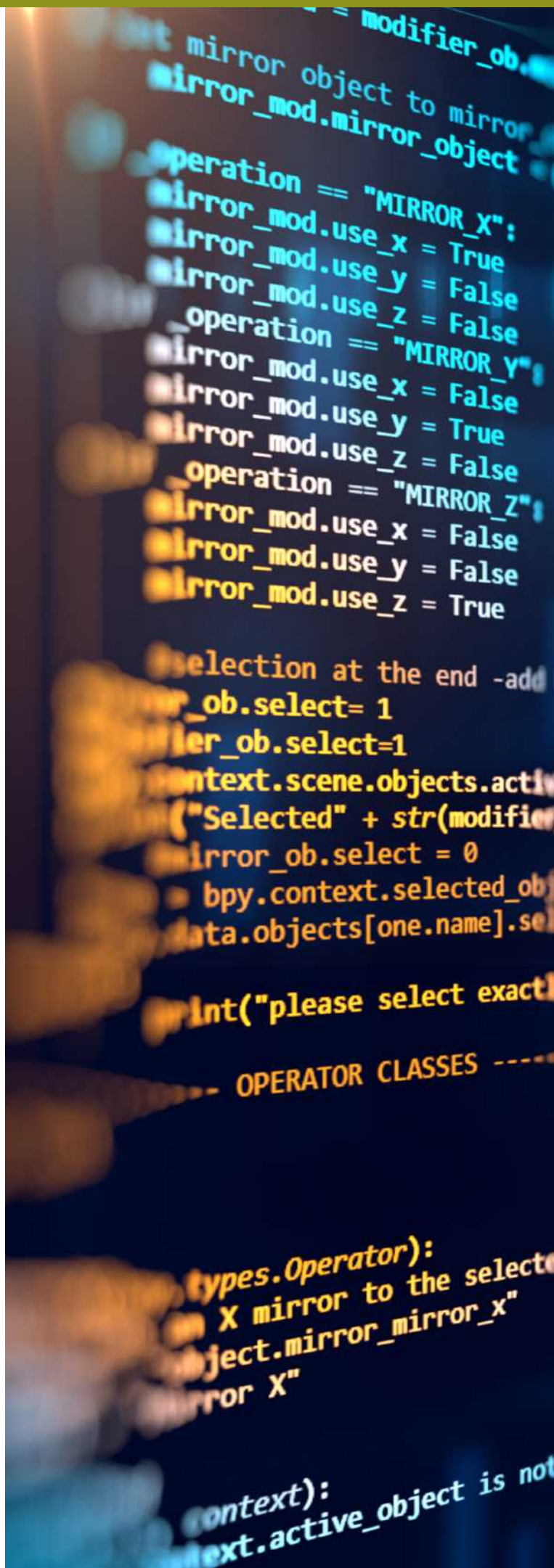
2020 (or 2021) will finally see Australia's defamation laws upgraded to deal with the new digital world, both in case law as well as in legislation. There are further reforms on the horizon too, dealing with liability of online platform providers such as Google, and many hope reforms will address issues raised by the *Voller* decisions.

In the meantime, those whose business activities expose them to defamation claims should be keenly aware of the high financial risks (and impacts on reputation and resources) these claims pose. Businesses should also be aware of the ever-increasing avenues by which liability may arise, and should implement appropriate policies and procedures to help mitigate this risk as outlined above.

Author
Peter Stokes
Partner - Litigation and Dispute Resolution

Author
Rebecca Lindhout
Special Counsel - Digital and Intellectual Property

Author
Lornagh Lomax
Lawyer - Digital and Intellectual Property



Smart(er) contracts in 2020

Blockchain well and truly entered into the vernacular during the 'ICO boom' of 2017, and for many the term has become synonymous with cryptocurrency. Although very much still in development, blockchain technology has the potential to move beyond simply recording and verifying transactions. In particular, there has been a renewed interest, and increased experimentation, in codifying legal agreements on blockchains through the use of smart contracts.

This article discusses some of the current opportunities and challenges facing the adoption of blockchain technology, and in particular smart contracts.

WHAT IS A BLOCKCHAIN?

Blockchains are tamper resistant digital ledgers implemented in a distributed fashion, usually without a central authority. This distributed ledger system essentially takes a number of records and bundles them into data sets or 'blocks'. That block gets chained to the next block using a cryptographic signature or 'key'. The blockchain then acts as a ledger and the keys control who can do what within the ledger. Each user owns a full copy of the ledger, and plays an important role in automatically and continuously agreeing on the current state of the ledger and all of the transactions recorded in it. Blockchains can be public (i.e. anyone can become part of the network) or private (i.e. only approved participants can become part of the network).

At their most basic level, a blockchain enables a community of users to record transactions in the ledger that is public to that community, such that, effectively, no transaction can be changed once published. It is the data transparency between all users in the network, and underlying cryptography, that removes the need for a trusted intermediary.

WHAT ARE SMART CONTRACTS?

The term smart contract is something of a misnomer. As Ethereum founder Vitalik Buterin tweeted in 2018, they should have been called "something more boring and technical, perhaps something like persistent scripts". A smart contract is a self-executing, self enforcing protocol which is governed by its explicit terms and conditions. To enter into a blockchain based smart contract, the parties first negotiate and agree to the terms of the agreement before memorialising the terms (either in part or entirely) in smart contract code.

Matters which utilise clear rules and quantifiable terms of engagement are well suited to implementing smart contracts. For example, blockchain and smart contract technology is already being utilised:

- in the logistics sector – to shorten the chain of third party agents, shorten delivery timeframes, track the transportation of goods and potentially reduce the price to consumers and chances of theft;

- in the food and wine sector – to track the provenance of products to better prevent food fraud; and

- in the financial services sector – the opportunities are almost endless for financial services and include, for example, payment processing (including cross-border payments), clearing and settlement of financial instruments, trade finance and automated over the counter (**OTC**) derivatives contracts, as well as regulatory technology such as streamlined 'know your customer' certification.

ADVANTAGES OF USING SMART CONTRACTS

There are a number of common advantages which smart contracts can offer. These include:

Accuracy and transparency: As the codified terms are fully visible and accessible to all relevant parties, there is no way to dispute them once the smart contract is established. This facilities complete transactional transparency and removes (or, at the very least, reduces the likelihood) of any manipulation, bias or error which in turn encourages greater confidence in the execution of the smart contract. This, in turn leads to decreased monitoring costs and risks of opportunistic behaviour.

Efficiency: Smart contracts are able to improve the efficiency with which commercial arrangements are carried out due to:

- automated execution;

- the bypassing of bureaucratic mechanisms;

- the high speed of execution thanks to the use of mathematical algorithms in blockchain applications instead of bureaucratic mechanisms;

- there being no requirement to process documents manually; and

- a lack of miscommunication due to the explicit nature of the codified terms.

Many smart contract-proposed use cases assume that the smart contract will receive information or parameters from 'off-chain' resources. This can cause two major issues. Firstly, smart contracts do not have the ability to pull data from off-chain resources; rather, the information must be 'pushed' to the smart contract. Secondly, if the data at issue is in constant flux, and since the code is replicated across multiple nodes, different nodes across the network may be receiving slightly different information. As consensus is required across the nodes for a transaction to be validated, these fluctuations may prevent the condition from being satisfied. Contracting parties can, however, solve this issue in a streamlined and transparent way by using an 'oracle'. Oracles are trusted third parties (which may be software or actual people) that retrieve off-chain information and then push that information to the blockchain at predetermined times.

Security: Smart contracts are afforded the reliability and tamper-resistant nature of the decentralised data storage which underpins blockchain technology. In particular, because of the distributed nature of a blockchain, along with consensus mechanisms and hashing algorithms, once information has been recorded to a blockchain, it becomes incredibly hard to change or delete. A party does not have the ability to modify or roll back information stored on a blockchain, or halt the execution of a smart contract once it has been deployed, unless provided for in the code.

LEGAL AND REGULATORY CHALLENGES OF SMART CONTRACTS

Despite the opportunities the adoption of smart contracts can offer, there are still a myriad of issues, including, in particular, legal and regulatory challenges, which are preventing the more widespread utilisation of smart contracts. These include:

Interpretation and enforceability: If there is a dispute about whether a smart contract accurately memorialised the parties' intentions or whether one party has breached the contract, the parties may still bring legal proceedings or engage in alternative dispute resolution processes. As contract law varies between different jurisdictions, so too will the enforceability of smart contracts depending on any formal requirements required in a particular jurisdiction.

Assuming the smart contract is enforceable, how then do the parties to the contract, a judge or a regulator interpret the terms that are written in code? While judges may not look to sources external to the contract to interpret the code, natural language clauses can be linked to the digital clauses for interpretation purposes. These hybrid contracts are referred to as 'Ricardian contracts'. Coding within the blockchain ledger contains a reference to the natural language clause thereby incorporating it into the digitised contract. If all goes smoothly, it may be that the natural language clauses will not need to be referred to.

If a different outcome was mandated by law, how would a smart contract transaction on the blockchain be unwound? And what would that mean for the downstream transactions that have already formed on the blockchain? Will there be a need to legislate for 'kill switches' in times of stress?

Liability and risk allocation: Smart contract 'purists' take the view that the smart contract code should simply resolve issues of liability through performance. However, this is a simplistic view. There will always be interests that differ between two counterparties, regardless of the assumptions on which the technology is built and runs. This is a reality of trade and commerce, and means that it is not possible to escape the fact that there may need to be adjudication on matters of liability.

Smart contracts also introduce a completely novel risk that the contract will be hacked or that the code or protocol simply contains an unintended programming error. In relation to blockchain technology, these concepts are closely aligned as most hacks associated with blockchain technology eventuate from exploitations of an unintended coding error. Parties to a smart contract will need to consider how risk and liability for unintended coding errors and resulting exploitations ought to be allocated between the parties, and possibly with any third party developers or insurers of the smart contract. For example, the parties may seek written representations from the programmer that the code performs as contemplated.

Confidentiality, security and privacy: Although the transparent nature of smart contracts is potentially advantageous, some smart contracts may exhibit a degree of transparency that is undesirable to some parties. Unlike traditional contracts, all transactions executed via a smart contract, are propagated across all of the nodes in the network, which creates privacy issues, particularly when the accounts of the parties are associated with known entities. Even when the parties are not identified (e.g. they rely on pseudonymous accounts), certain identification techniques can be used to discern the identities of parties who transact with a particular smart contract.

Interestingly, the flip side to the confidentiality/privacy debate is that the availability of the data provides an audit trail and a much more efficient way for regulators to view the information they need to ensure regulatory compliance – essentially, acting as a "regulatory app".

Jurisdictional issues: Smart contracts also raise interesting jurisdictional issues. Because blockchain operates as a decentralised ledger, it means that smart contracts can be formed and accessed anywhere across the globe. They do not reside in any one location, but exist across multiple locations at the one time. Yet our laws are jurisdiction-based.

The differences in laws across jurisdictions – including matters as basic as ownership – can be highly problematic, resulting in incongruent rights and responsibilities, and confusion regarding the consequences if there is a contract violation.

Evidentiary matters: As smart contracts begin to proliferate, they will be subject to examination. This means there will be a need for new types of cryptography experts, and forensics experts, to verify software code and to translate the code into human-readable form.

Regulated contracts: Smart contracts sit uneasily with certain types of regulated contracts. Take, for example, Australian unfair contract terms legislation. A contract written in code is probably not going to be sufficiently transparent for the purposes of informing a consumer or small business.

Regulatory and policy settings: Existing regulatory and policy settings will need to be considered in greater detail. How are regulators to police smart contracts? And what opportunities exist for parties to use the technology to potentially side-step the law by hiding the identity of the parties and the governing jurisdiction of the contract? How are cross-jurisdictional issues of taxation, national security and anti-money laundering to be managed?

WHERE TO FROM HERE FOR AUSTRALIA?

In addition to the release of the National Blockchain Roadmap in February 2020, several Australian Government agencies have sought to clarify the regulatory issues that affect the implementation and use of blockchain. For example:

- the Australian Securities and Investments Commission has released guidance in relation to when the use of blockchain technology may attract regulation under Australian financial services regulatory laws (for example, when an initial coin offering may constitute an offer of shares or interests in a managed investment scheme);

- the Australian Taxation Office has also released guidance in relation to the tax treatment of digital assets;

- following legislative changes in 2018, digital currency exchange operators with a geographical link to Australia are now required to comply with Australian anti-money laundering and counter-terrorism financing laws;

- the Federal Government has provided funding to Standards Australia to develop, in concert with the International Organization for Standardization, international blockchain standards; and

- IP Australia co-leads the Committee on World Intellectual Property Organization Standards Blockchain Task Force, which is exploring the potential of blockchain technology for the IP Rights ecosystem.

The Australian Government has acknowledged that there are many opportunities blockchain technology and particularly smart contracts can facilitate across various sectors, however, Australia's ability to capitalise on these opportunities will depend (at least in part), upon effective, efficient and appropriate regulation and standards.

Author
Matthew McMillan
Partner - Digital and Intellectual Property

Author
Trudi Procter
Partner - Financial services regulation (including fintech and regtech)

Author
Rebecca Lindhout
Special Counsel - Digital and Intellectual Property

Author
Kathryn Morgan
Senior Associate - Financial services regulation (including fintech and regtech)

COVID-19 and the new digital clinical trial era

The era of the digital clinical trial may already be upon us thanks to the impacts of COVID-19. While conceptualisations of the 'digital patient' and technology-integrated clinical trials were somewhat futuristic even in 2019, with COVID-19 grinding clinical trials to a halt in 2020, the life sciences industry may be forced to pivot into this conceptualised digital era much faster than anticipated – and, unlike most COVID-related impacts, this isn't bad news. While this presents an exciting opportunity for life sciences and bio technology stakeholders to digitally innovate the clinical trial process, steps toward digital innovation should be matched with increased attention to regulatory caveats, patient privacy and data protection.

COVID-19 AND THE REQUIREMENT TO THINK DIFFERENTLY AND *DIGITALLY*

COVID-19 has impacted clinical trials globally. Border restrictions are preventing patient access to trial sites, there is increased concern from patients about exposure to COVID-19, trial drug supply chains are being interrupted and medical resources and personnel involved in clinical trials are being reallocated to the pandemic's front line. In response, international and domestic regulatory bodies are publishing guidance on alternative models and approaches for conducting clinical trials. This guidance has largely included using *technology* to overcome COVID-induced obstacles.

For example, in the United States, the Food and Drug Administration (**FDA**) is encouraging sponsors, clinical investigators and Institution Review Boards to consider adopting altered policies and procedures regarding informed consents, study visits and procedures, data collection, study monitoring and adverse event reporting in clinical trials.

AUSTRALIA'S STANCE

In Australia, the Australian National Health and Medical Research Council (**NHMRC**) has released the *COVID-19: Guidance on clinical trials for institutions, HRECs, researchers and sponsors* (**Guidance**). The Guidance outlines that employing digital strategies to continue clinical trials during COVID-19 is acceptable, and now *encouraged*, where certain approvals are obtained.

Practically this looks like using strategies to gain pre-approval for certain categories of amendments to clinical trials, including:

- allowing virtual visits by patients;
- employing telehealth – providing telemedicine and medical education via digital means;
- using electronic consents for trial participation;
- using other means to implement teletrials;

- changing the trial 'site' to a location outside of a hospital or clinic (and using digital platforms to transmit results and research); and

- broadly, any other changes that do not implicate participants' safety or well-being and are intended for the purpose of safeguarding the health of participants, researchers and staff or the community via infection control or the burden of participation in a trial for the participant or researchers.

The last broad suggestion by the NHMRC in particular opens the door for technology and life sciences industries to collaborate and create innovative ways to use technologies in clinical trials, as long as they safeguard health, protect against infection and reduce the burden of participation in clinical trials during COVID-19.

While using digital technologies in Australian clinical trials must be seemingly COVID-related for now, we consider this digital shift may well be the catalyst for the era of a digital clinical trial in a post-COVID world.

WHAT THIS MEANS – DIGITALISATION IN CLINICAL TRIALS

Technology has already revolutionised many industries. In the travel, banking and retail industries, digitisation has changed the ways we hail transport, conduct banking transactions and shop. Similarly, in the life sciences space, digital intervention in clinical trials could mean:

- de-centralised research and testing resulting in access to broader demographics using remote trial locations;

- improved patient experiences and therefore increased patient trial participation and retention;

- more accurate and real-time data collection; and

- expedited trials.

Faster trials may mean faster concept-to-market timeframes for in-demand medicines and treatments.

Moreover, the acceptance of teletrials, digital apps for patient-to-trial matching, e-consents and the use of wearables and smart devices for data collection and sharing into clinical trials could open the door for biotech's to plug large (and arguably 'Analog Age') deficiencies in existing clinical trial processes.

PRIVACY AND DATA PROTECTION

As demand for digital solutions increases in 2020 and beyond, those involved in manufacturing, supplying or implementing medical technologies need to be keenly aware of, and implement, privacy and data protection processes and strategies.

By nature, data collection and exchange in clinical trials involves sensitive patient information. Securing protection of this data is crucial to building patient trust and creating a sustainable digital infrastructure.

FINAL THOUGHTS

COVID-19 is forcing regulatory bodies and medical research stakeholders to think laterally to overcome pandemic-induced obstacles to clinical trial progress. While we may not see a digital overhaul in clinical trials immediately, we do consider that COVID-19 and the need to pivot will see a digital shift in the life sciences industry permanently.

With this, we expect greater collaboration between the technology and life sciences industries. In order to be successful, however, we consider parties hoping to capitalise on this digital opportunity in clinical trials will need astute understanding and implementation of privacy and data protection.

Author
Belinda Breakspear
Partner - Digital and Intellectual Property

Author
Jake Grant
Special Counsel - Digital and Intellectual Property

Author
Lornagh Lomax
Lawyer - Digital and Intellectual Property

Watch this space: *keeping you informed on the latest TMT news and trends*

Twitter outage linked to data breach

On 15 July, Twitter announced that it had suffered a data security breach, which allowed the accounts of various world leaders and prominent individuals to be compromised. As part of its response to the breach, it shut down all 'blue tick' verified accounts for about an hour, which naturally triggered worldwide attention to the issue.

While according to Twitter's own blog update, it is still investigating the issue, we know already a reasonable amount about what happened. To this end, it is a very timely reminder of the risks of social engineering, when even one of the world's leading technology companies can have its two-factor authentication measures bypassed. It will also be interesting to see what comes from the inevitable investigations and notifications – it appears that personal information was compromised and so data breach notification laws globally (think Californian Civil Code in the USA, General Data Protection Regulation (**GDPR**) in Europe, Privacy Act in Australia and beyond) may have been triggered.

SO WHAT HAPPENED?

In short, attackers targeted certain Twitter employees through a social engineering scheme and gained their login credentials. With those credentials, they were able to then access Twitter's internal systems and use some internal support tools to compromise live Twitter accounts.

About 130 accounts were targeted, and of these, 45 were compromised to the extent that the passwords were reset, and the attackers gained full access of the accounts.

Once they had access, the attackers started posting public requests for bitcoin payments from those accounts (which received responses, perhaps surprisingly), and it is thought that this financial motivation is the key reason behind the attacks. The FBI is reportedly investigating the data breach, as is Twitter of course, and while it appears at the moment that only accounts that had the bitcoin message were taken over, but it might be more widespread than that.

It is quite extraordinary to think that verified accounts could be compromised in this way. With access to the accounts, contact details and the substance of messages (including all DMs) has been compromised and may (likely) have been copied. If that is the case, not only does it raise the issue of privacy-related data breach notification, but perhaps more significantly, raises risks around the misuse of commercially sensitive information, or even information relating to matters of national (or international) security, which could have been present in those compromised messages.

Beyond that, there are broader questions being raised about how Twitter's platform operates. From screenshots of the admin module allegedly obtained from the attackers, there are suggestions that Twitter's platform does not simply display messages unthinkingly, but that there is scope for Twitter to curate trends or hide users or tweets from showing up in searches. If that were ultimately the case, it would be highly significant because it is contrary to how Twitter has publicly explained its platform, and might impact on the conclusions reached in the US Department of Justice's current examination of whether to strip Twitter and Facebook of their immunity from slander laws as mere information conduits rather than publishers.

There is plenty more to come from this story – watch this space.

Author
Alex Hutchens
Partner - Digital and Intellectual Property

2020 Media law reforms in Australia

Just over one year after the Australian Competition and Consumer Commission (**ACCC**) released its *Digital Platform Inquiry – final report*[1] (**DPI**), Australia's media regulatory landscape is finally set for a shake up, with reforms to address largely unregulated online media platforms anticipated for late 2020.

DRAFT MANDATORY CODE OF CONDUCT DUE JULY 2020 – NEWS MEDIA AND ONLINE PLATFORMS

After public consultation and despite pushback from Facebook and Google, the ACCC is due to release a draft mandatory code of conduct (**Code**) by the end of July 2020 to govern commercial relationships between large digital platforms and news media companies. This is just weeks after Google announced it would launch a licensing program to pay publishers for high-quality content for a 'new news experience'.

The Australian Government directed the ACCC in April to draft the mandatory Code after tech giants, Google and Facebook, failed to negotiate voluntary codes of conduct with media outlets, as requested under the Government's formal *Response*[2] to the DPI.

The mandatory code is anticipated to address concerns around:

- data sharing;
- ranking and display of news content; and
- monetisation and the sharing of revenue generated from news.

The Code is also set to establish appropriate enforcement, penalty and binding dispute resolution mechanisms.

Whether large digital platforms will bow to the pressures of the Australian Government once a Code is introduced is yet to be seen, however Google's proposed licensing program is a step towards suggesting a compromise.

PUBLIC CONSULTATION HAS ENDED FOR PROPOSED 'PLATFORM NEUTRAL' REFORM OPTIONS TO THE FILM, TELEVISION AND BROADCASTING INDUSTRY

Earlier this year and in response to the DPI, the Australian Government, in conjunction with Screen Australia and the Australian Communications and Media Authority (**ACMA**), released its *Options Paper* on how to best support Australian stories in a modern, multi-platform media landscape. With submissions now closed, Australia is one step closer to 'platform-neutral' media regulation as the government deliberates on how best to move forward.

The Options Paper proposed effectively four potential reform models:

- maintain the status quo – no changes;
- fine tune the existing regulatory framework and incentives;
- significantly overhaul the regulatory framework to create platform-neutral regulation for both traditional broadcasters and online platforms; or
- completely deregulate the media industry so that no media platform is subject to regulation.

The models discussed options for:

- minimum expenditure and distribution quotas for local content across each platform;
- reworking the Producer, Location and Post, Digital and Visual Effects (**PDV**) Offset percentages, as well as the future of the Location Incentive; and
- discoverability requirements for Australian content on subscription video on demand (**SVOD**) services.

The Options Paper received over 300 responses from various stakeholders, with broad support ranging from complete deregulation and scrapping of sub-quotas, to modified versions of deregulation to support for equal regulation standards across all media platforms. Netflix also proposed a flexible, reasonably set voluntary investment model that would meet 'cultural policy goals and incentivises wider investment' instead of imposing a quota system on SVOD services.

The ACCC and Australian Government are yet to comment on next steps after submissions closed on 3 July 2020.

Despite wide-ranging debate over the best way forward for media regulation reform in Australia, most stakeholders are urging the Australian Government to stick to its planned time frame to initiate reform in 2020. We anticipate a government response in the coming months, and consider a draft reform plan may look like a combination of model 3 and model 4. The media regulatory landscape may look very different heading into 2021.

FOOTNOTES: 1. Digital Platforms Inquiry – final report (2019), Australian Competition and Consumer Commission, published 26 July 2019. | 2. Government Response and Implementation Roadmap for the Digital Platforms Inquiry (2019), Australian Government, published 12 December 2019.

Author
Belinda Breakspear
Partner - Digital and Intellectual Property

Author
Lornagh Lomax
Lawyer - Digital and Intellectual Property

Kangaroos and cowboys

Most people will have heard of a 'bull market' or a 'bear market', but United States (**US**) business news provider CNBC added a new animal to the financial zoo earlier this year by describing the current US stock market as a 'kangaroo market' (due, presumably, to its bouncing up and down without any specific trend).

This unprecedented volatility has been attributed, at least in part, to the rise of investment apps and particularly zero-commission trading apps in the US. Robinhood, a particularly popular app, added a staggering 3 million users in the first quarter, while average daily trading volumes tripled. Similarly, competitors Charles Schwab, TD Ameritrade and ETrade added 1.5 million accounts (double the amount added in the previous quarter).

Although there are a number of investment apps available in the Australian market, at the time of writing this article, there are no zero-commission stock trading apps currently available. Despite this, a similar rush into the stock market by retail investors is occurring in Australia.

An analysis of markets by the Australian Securities and Investments Commission (**ASIC**) has revealed a substantial increase in retail activity across the securities market, as well as greater exposure to risk, during the COVID-19 pandemic period. ASIC found that trading frequency has increased rapidly, as has the number of different securities traded per day, and the duration for holding the securities has significantly decreased, suggesting an increase in short-term and 'day-trading' activity by retail investors.

In addition to the increased trading, there was a sharp increase in the number of new retail investors to the market, up by a factor of 3.4 times. ASIC has indicated they are also particularly concerned by the significant increase in retail investors' trading in complex, often high-risk investment products including highly-geared exchange traded products and Contracts For Difference (**CFDs**).

ASIC has published a report in response to these issues which highlights a range of potential retail investor harms identified by ASIC as a result of the increased market volatility during the COVID-19 pandemic period. More recently, ASIC has also released a new regulatory guide in relation to the administration of its product intervention power. ASIC has previously used its product intervention power to ban a short-term credit product and have consulted on the proposed use of its power to address other financial products, including over-the-counter (**OTC**) binary options and CFDs.

Introduced as part of the Government's response to the Financial System Inquiry, the product intervention power enables ASIC to make a product intervention order when a financial product or a credit product (or a class of such products) has resulted, will result or is likely to result in significant consumer detriment. As investment apps continue to grow in popularity, it will be interesting to see how ASIC will choose to manage these apps.

Author
Trudi Procter
Partner - Financial services regulation (including fintech and regtech)

Author
Tim Wiedman
Partner - Financial services regulation (including fintech and regtech)

Author
Kathryn Morgan
Senior Associate - Financial services regulation (including fintech and regtech)

ACCC commences proceedings against Google – consent in the spotlight

The Australian Competition and Consumer Commission (**ACCC**) launched proceedings in the Federal Court of Australia against Google for misleading Australian consumers about its privacy collection practices.

The ACCC alleges Google misled consumers when it failed to properly inform consumers, and failed to gain explicit informed consent, about its decision to combine personal information in consumers' Google accounts with information about those individuals' activities on non-Google sites to display targeted advertisements.

This meant this data about users' non-Google online activity became linked to their names and other identifying information held by Google, when this had not previously occurred. Armed with the newly linked data, Google was able to provide more effective targeted ads.

The ACCC also alleges that Google misled consumers about a related change to its privacy policy. Despite there being a pop up notice that purported to obtain the individuals' consent to the change in practice, the ACCC alleges that consent was not genuinely and freely given because individuals could not understand what implications flowed from the change, and that this also breached Google's own statement in its privacy policy that it would not make detrimental changes to its data handling practices without individuals' consent.

The case demonstrates the clear linkage between consumer protection law and privacy law, which is a theme arising from the ACCC's *Digital Platform Inquiry – final report*[1].

Of note, it is interesting that:

- the consumer protection regulator, the ACCC, is bringing the proceedings rather than the privacy regulator, the Office of the Australian Information Commissioner (**OAIC**). It is a consumer protection claim rather than a privacy claim, even though it relates to privacy practices;

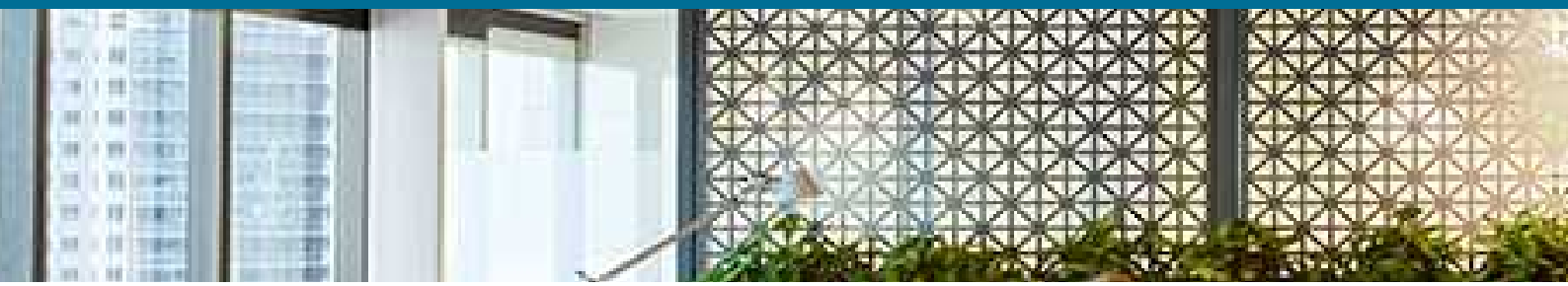
- the regulator considers that the 'price' paid for a service is data – which makes it explicitly the consideration for any contract formed, but simultaneously excludes that term from the unfair terms regime in Australia (potentially at odds with the CCPA in California which looks to enable customers to refuse to 'pay' with data);

- as a result of bringing the proceedings this way, the expanded enforcement and penalty regimes under the *Competition and Consumer Act 2010* are available (including a penalty of 10% of the economic value of the impugned conduct). The ACCC has alleged that the impugned conduct was designed to increase the value of Google's suite of services, so this is obviously a key consideration. By contrast, the maximum financial penalty under the *Privacy Act 1988* (Cth) is $2.1m for serious or repeated privacy breaches; and

- this case explores the efficacy of consent in an online environment. In the post-GDPR world, consent is an increasingly problematic basis on which to process data. However, privacy law is not the only relevant perspective here. In an online environment, consumer protection law makes unilateral changes to terms a potentially unfair term (subject of course to the note above about price not able to be an unfair term), and further, Google's own terms said that consent would be sought for any negative changes (possibly to deal with the unfair terms issue), but consent for those new collection practices may not actually have been required under Australia's privacy laws (consent is only required in very limited circumstances). Therefore, it will be complicated to work out how those competing perspectives on consent will be ultimately resolved and the Court's treatment of them will be very instructive across various spheres of online contracting.

FOOTNOTES: 1. Digital Platforms Inquiry – final report (2019), Australian Competition and Consumer Commission, published 26 July 2019.

Author
Alex Hutchens
Partner - Digital and Intellectual Property



Meet the team

Operating for over 94 years, McCullough Robertson is an independent, Australian law firm with a proven track record of providing a range of legal services to the TMT industries. 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

Alex Hutchens
Partner and Head of Technology, media and telecommunications
P +61 2 8241 5609
E ahutchens@mccullough.com.au

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

Belinda Breakspear
Partner and Head of Digital and Intellectual Property
P +61 7 3233 8968
E bbreakspear@mccullough.com.au

Paul McLachlan
Strategic Adviser
P +61 2 8241 5606
E pmclachlan@mccullough.com.au

Corporate Advisory and Taxation

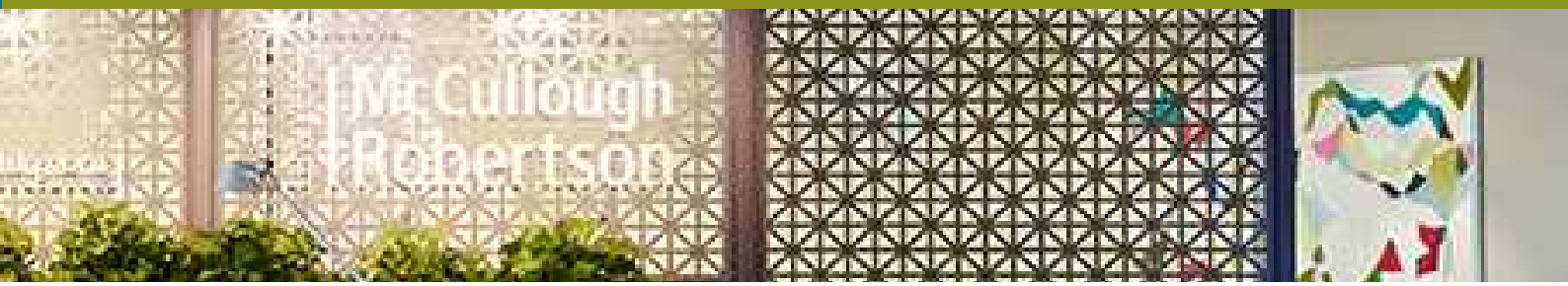
Reece Walker
Chairman of Partners and Head of Life Sciences
P +61 7 3233 8654
E rwalker@mccullough.com.au

John Kettle
Partner
P +61 7 3233 8962
E jkettle@mccullough.com.au

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

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

Adrian Smith
Partner
P +61 2 8241 5639
E adriansmith@mccullough.com.au



Financial Services Regulation

Trudi Procter
Partner
P +61 7 3233 8727
E tprocter@mccullough.com.au

Tim Wiedman
Partner
P +61 7 3233 8716
E twiedman@mccullough.com.au

Litigation and Dispute Resolution

Guy Humble
Partner
P +61 7 3233 8844
E ghumble@mccullough.com.au

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

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

Insurance and Corporate Risk

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

James Lynagh
Senior Associate
P +61 7 3233 8906
E jlynagh@mccullough.com.au

Property, Projects and Finance

Eva Vicic
Partner
P +61 2 8241 5634
E evicic@mccullough.com.au

Matt Bradbury
Partner
P +61 7 3233 8972
E mbradbury@mccullough.com.au

Jane Newman
Senior Associate
P +61 7 3233 8665
E jnewman@mccullough.com.au

Employment Relations and Safety

Scarlet Reid
Partner
P +61 2 8241 5688
E sreid@mccullough.com.au

Nathan Roberts
Senior Associate
P +61 2 8241 5694
E nroberts@mccullough.com.au

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