2022 . Vol 25 No 2

Contents

page 18 **The role of defamation in Australia: developments in the legal and regulatory landscape continue to shape the approach to online content**
Julian Lincoln, ***Audrey Vong*** *and* ***Kathryn Quinn***
HERBERT SMITH FREEHILLS

page 22 **Greater regulation for crypto exchanges may be on the horizon**
James North, ***Steven Rice***, ***Lachlan Ellison*** *and* ***Javier Cross*** *CORRS CHAMBERS WESTGARTH*

page 26 **Cybercrime — an Australian overview**
Dennis Miralis, ***Lara Khider*** *and* ***Mohamed Naleemudeen*** *NYMAN GIBSON MIRALIS*

page 29 **The Google/Barilaro fiasco!**
Patrick George *KENNEDYS*

The role of defamation in Australia: developments in the legal and regulatory landscape continue to shape the approach to online content

***Julian Lincoln**, **Audrey Vong** and **Kathryn Quinn** HERBERT SMITH FREEHILLS*

Introduction

Over the past year, there have been significant legal and regulatory activity globally in relation to digital platforms, online content and the associated risks and harms. In Australia, due to its consideration of serious harm to a person's reputation, defamation has become a prominent feature of such discussion alongside online harm and privacy, which has spanned from a number of parliamentary hearings[1] and other federal and regulatory activities, all of which has led to proposals for or enactment of new laws. Recent developments regarding defamation, specifically in online contexts, including case law and potential reforms, have only underscored the importance of considering how defamation is shaping the dissemination of online content on digital platforms in Australia.

What legal and regulatory developments have taken place over the past year?

Since 2005,[2] defamation in Australia has been governed by uniform Model Defamation Provisions (MDPs)[3] at the state and territory levels. In July 2021, following a review of MDPs,[4] changes to defamation laws[5] were introduced in Victoria, NSW, South Australia and the Australian Capital Territory. This was intended to refresh the outdated defamation regime, ensuring it could operate more efficiently and productively including in online contexts — unsurprisingly, given defamation has been at the forefront of conversations about potential harms from and liability for comments on social media and online news publications. However, the discussion about these reforms garnered complex feedback in relation to digital platforms and preceded the Australian Competition and Consumer Commission's (ACCC) digital platforms inquiry final report. As a result, the second stage of review of MDPs is now underway[6] and seeks additional input regarding the categorisation of treatment of internet intermediaries. This second stage of review may have significant implications for which parties bear liability for defamatory material in the online context in Australia.

In the courts, the recent and highly publicised High Court decision of *Fairfax Media Publications Pty Ltd v Voller*[7] (*Voller*) and the continuing *Defteros v Google LLC*,[8] *Defteros v Google LLC (Costs)*[9] and *Defteros v Google LLC*[10] (collectively referred to here as *Defteros* cases), play a crucial role in determining how defamation operates on digital platforms, most notably by determining what it means to be a "publisher" of defamatory material online.

Defteros considers whether a search engine can be liable for defamatory content that appears in its search results. In 2020, Mr George Defteros brought a defamation claim against Google for failing to remove the hyperlink in its search results to a news article published by *The Age* on 18 June 2004, which defamed Mr Defteros.[11] The Victorian Supreme Court found that, after the complainant made Google aware of the hyperlink leading to defamatory materials, Google was liable; in June 2021 the Victorian Court of Appeal affirmed this decision.[12] The High Court will soon make a final determination of whether Google is classed as a "publisher" of content appearing on its search results page by virtue of providing a hyperlink to defamatory material. If Google is found to be a publisher as such, there would be a significant shift in how search engines can operate and disseminate online content in Australia: they would need to constantly monitor and remove, or otherwise potentially assume liability for, any defamatory content indexed and linked in their search results pages.

In *Voller*, the High Court found that media companies could be held responsible as "publishers" of allegedly defamatory comments posted by third-party Facebook users on the Facebook pages of media companies. The

High Court's reasoning centred around the fact that media companies chose to create their own Facebook pages and allow Facebook users to post publicly visible comments on their Facebook pages in response to content posted by the media companies themselves; they were therefore encouraging, facilitating and assisting the publication of the defamatory comments made by others.[13]

The federal government introduced an exposure draft of the Social Media (Anti-Trolling) Bill 2021 (Cth)[14] (Anti-Trolling Bill) less than 3 months after the *Voller* decision was handed down.[15] The stated intent of the Anti-Trolling Bill was to urgently address the High Court's determination regarding publication of defamatory comments on social media and to protect Australian organisations and individuals on social media from liability for anonymous defamatory comments on their social media pages. Principally, it aimed to accomplish this by introducing powers to "unmask" anonymous commenters by requiring social media providers to obtain their contact details for the purpose of bringing defamation proceedings and imposing liability for such defamatory comments on social media service providers if they did not fulfil certain requirements and introduced processes to fulfil such obligations.[16]

In addition to the newly proposed Anti-Trolling Bill, the federal government also recently enacted a new online safety regime.[17] The Online Safety Act 2021 (Cth) is focused on online harmful content (for example, cyberbullying material targeted at children and cyber abuse material targeted at adults)[18] as distinct from defamatory material and was stated to have been designed to operate harmoniously with Australian defamation laws.

However, there is potential significant overlap between the applications of both regimes in addressing the potential harms resulting from online content.

What are the implications of recent legal and regulatory developments and what are we likely to see next?

Legal and regulatory activity surrounding defamation on digital platforms and in online contexts is unlikely to slow down as new challenges in digital and online environments continue to arise.

Following the election of the new Labor Federal Government in May 2022, in the second half of 2022 and beyond, we are likely to see the new government begin to establish its regulatory priorities, as well as the decisions in *Defteros* and similar cases. In parallel, the second stage of the MDPs review is continuing, and discussions around long-awaited privacy reforms may offer valuable lessons in how regulation is developed and applied in relation to digital platforms and online content.

Having been introduced in the months preceding the 2022 election, the Anti-Trolling Bill lapsed at the dissolution of Parliament in April 2022. Prior to that, responses received by the Inquiry Committee[19] were critical of the overall regulatory intent and proposed mechanisms of the Anti-Trolling Bill. Although it was widely discussed as combatting "trolling", the Anti-Trolling Bill narrowly dealt only with anonymous comments in relation to defamation proceedings (the requirements of which may be unclear or inaccessible to the general public); furthermore, it only applied to "social media services",[20] meaning many other digital platforms (such as search engines) would not have been captured.

The *Voller* decision and the lapsing of the Anti-Trolling Bill have potentially opened the door for any organisation or person with a public social media page to be liable for publishing defamatory comments of third parties online, regardless of whether the organisation or person is aware that the comment exists. Furthermore, while the High Court's determination of the circumstances of publication stands, the case was ultimately settled before it returned to the NSW Supreme Court, where it is likely the defence of innocent dissemination would have been tested.

It is clear that legal and regulatory developments related to defamation in digital contexts can rapidly affect the ways in which online content is disseminated and managed in Australia. Following *Voller*, several politicians and other high-profile individuals turned off comments on their Facebook pages[21] for fear of being held liable for defamatory comments made by third parties. Beyond the High Court's impending decision in *Defteros*, going forward, we are likely to see defamation cases which continue to test the scope of those who may be liable as publishers of defamatory material online. In June 2022, the Federal Court of Australia found Google liable for user-generated videos posted on YouTube that were defamatory of former NSW Deputy Premier, John Barilaro.[22] The court held that Google became liable as a publisher of the defamatory videos at the point after which YouTube had been made aware of their existence, reviewed the content which was clearly defamatory and did not take the videos down.

In a similar vein, the second stage of the MDPs review will also consider whether an internet intermediary (an entity that provides services to facilitate use of the internet) should be liable for the defamatory conduct of third parties. The shifting scope of liability for and requirements in relation to defamatory material, along

with parallel obligations imposed by online safety and privacy regimes on the same online content and services, may make it increasingly difficult for digital platforms and other technology companies to stay abreast of and operate in accordance with their obligations in Australia.

Finally, consideration of defamation reforms relating to the online context of the second stage of the MDPs review may be able to incorporate valuable lessons from the development of online safety and online privacy reforms. The past year also featured consultations on long-awaited privacy reforms, with not only a Discussion Paper on a review of the Privacy Act 1988 (Cth), but also the introduction of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (Cth) (Online Privacy Bill), which focused on privacy in the online context. The government's approach to treating privacy and online privacy legislation separately has revealed the complexities of enacting separate legislation with overlapping regulatory intent, with some criticisms that the Online Privacy Bill is overly specific to online settings and was not well aligned with wider privacy law reform.[23] It also contained highly specific measures aimed at protecting children in online settings, overlapping with the goals and requirements of the new online safety regime — which, in turn, may also consider defamatory online content.

Looking ahead to a balanced approach to the development of defamation law in online contexts

As the digital landscape continues to increase in breadth and complexity, the defamation regime in Australia will no doubt continue to evolve in response. However, without a considered and nuanced approach to the interaction between the two areas, there is a risk of disproportionately or inappropriately relying on defamation in the regulation of online content, or for developments in defamation law failing to keep up with the reality of digital environments.

These regulatory challenges are neither unprecedented nor unfamiliar. We have already begun to see this balancing act play out in Australia as both privacy and online safety legislation contemplate parallel measures that may overlap in effect, if not in method, with the common end goal of protecting Australians from potential harms in the current online ecosystem. In other areas where regulation has struggled to keep pace with emerging technologies, we have seen the hurried introduction of regulatory safeguards that are limited to certain applications or use cases most subject to public scrutiny at the time (as with AI and facial surveillance technologies) — with slower responses to calls for the introduction of overarching regulatory frameworks.

Similarly, it is becoming clear that governments and regulators will need to consistently ensure that regulation aimed at online content is (and remains) fit for purpose and proportionate to harms, avoids fractured development and supports continued innovation. In Australia, developments in defamation law are another notable piece of the expanding regulatory framework to protect Australians from potential harms in the online landscape. If regulation is introduced in a piecemeal or unpredictable manner, this may be detrimental to the regulatory goals at hand, as well as creating uncertainty regarding legal and compliance obligations and impeding the development of best practices in relation to how organisations and individuals engage with online content. From a practical perspective, the global nature of online content also presents particular regulatory challenges: there is likely to be a push to harmonise standards and practices across different jurisdictions, especially on major digital platforms, and a highly specific regime reliant on defamation law means a risk of being significantly out of alignment with influential markets such as the EU.

The new federal government will no doubt have its regulatory priorities in the dissemination of, access to and harm prevention in relation to online content. In doing so, we suggest that it should carefully examine the development and critiques of the Anti-Trolling Bill and other legislative reforms in relation to online spaces, as well as the goals of those frameworks in concert with those of defamation law and reform in Australia. As the digital environment continues to evolve at a rapid pace, we should grasp the opportunity to refine our understanding of defamation in online contexts and ensure it is part of a harmonised and considered regime of online content regulation.

Julian Lincoln
Partner
Herbert Smith Freehills
Julian.Lincoln@hsf.com
www.herbertsmithfreehills.com

Audrey Vong
Solicitor
Herbert Smith Freehills
Audrey.Vong@hsf.com
www.herbertsmithfreehills.com

Kathryn Quinn
Solicitor
Herbert Smith Freehills
Kathryn.Quinn@hsf.com
www.herbertsmithfreehills.com

Footnotes

1. For example, the public hearings that formed part of the inquiry into social media and online safety.
2. Explanatory Note, Model Defamation Provisions 2005, https://pcc.gov.au/uniform/2020/Original_Model_Defamation_Provisions_2005.pdf.
3. Parliamentary Counsel's Committee *Model Defamation Provisions* (2020) https://pcc.gov.au/uniform/2020/Consolidated_Model_Defamation_Provisions.pdf.
4. O Griffiths "Reform of defamation law" *Law and Bills Digest* www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook46p/DefamationReform.
5. Explanatory Note, Model Defamation Amendment Provisions 2020.
6. NSW Government *Review of Model Defamation Provisions-Stage 2* Discussion Paper www.justice.nsw.gov.au/justicepolicy/Documents/review-model-defamation-provisions/discussion-paper-stage-2.pdf.
7. *Fairfax Media Publications Pty Ltd v Voller* (2021) 392 ALR 540; [2021] HCA 27; BC202108345.
8. *Defteros v Google LLC* [2020] VSC 219; BC202003565.
9. *Defteros v Google LLC (Costs)* [2020] VSC 324; BC202004866.
10. *Defteros v Google LLC* [2021] VSCA 167; BC202105158.
11. Above n 9.
12. Above n 10.
13. Above n 7, at [55].
14. Office of the Australian Information Commissioner, Exposure Draft to the Social Media (Anti-Trolling) Bill 2021 (Cth), www.oaic.gov.au/engage-with-us/submissions/exposure-draft-social-media-anti-trolling-bill-2021.
15. Legal and Constitutional Affairs Legislation Committee *Social Media (Anti-Trolling) Bill 2022 [Provisions]* (2022) https://parlinfo.aph.gov.au/parlInfo/download/publications/tabledpapers/c43c1a6a-d02e-4c18-b003-eee35fc76c8b/upload_pdf/Social%20Media%20(Anti-Trolling)%20Bill%202022%20[Provisions].pdf.
16. Attorney-General's Department, Social Media (Anti-Trolling) Bill, www.ag.gov.au/legal-system/social-media-anti-trolling-bill.
17. Online Safety Act 2021 (Cth).
18. Above n 15, ss 6 and 7.
19. Submissions to the Senate Standing Committee on Legal and Constitutional Affairs, *Social Media (Anti-Trolling) Bill 2022 [Provisions]* www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Anti-Trolling/Submissions.
20. In s 13(1) of above n 15, a "social media service" means (a) an electronic service that satisfies the following conditions: (i) the sole or primary purpose of the service is to enable online social interaction between two or more end-users, (ii) the service allows end-users to link to, or interact with, some or all of the other end-users, (iii) the service allows end-users to post material on the service, and (iv) such other conditions (if any) as are set out in the legislative rules; or, (b) an electronic service specified in the legislative rules.
21. J Taylor "More public figures expected to turn off Facebook comments after Australian defamation ruling" *The Guardian* 27 September 2021 www.theguardian.com/law/2021/sep/27/high-court-ruling-on-third-party-social-media-to-see-widespread-shutdown-of-comments-expert-says.
22. *Barilaro v Google LLC* [2022] FCA 650; BC202205103.
23. Attorney-General's Department, Online Privacy Bill Exposure Draft, https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/consultation/published_select_respondent.

Greater regulation for crypto exchanges may be on the horizon

James North, Steven Rice, Lachlan Ellison *and* ***Javier Cross*** *CORRS CHAMBERS WESTGARTH*

Key takeaways

- The Treasury is now considering submissions relating to a proposed licensing regime for crypto asset secondary service providers (CASSPrs), which would impose similar licensing and custody obligations to the Australian Financial Services Licence (AFSL) regime.
- The proposal broadens the scope of organisations which would be subject to such a regulatory framework compared to previous inquiries. The framework would apply not only to crypto exchanges, but to any platform which facilitates the exchange, storage or transfer of crypto assets.
- Platforms which hold private keys to crypto assets on behalf of their customers would be subject to further obligations relating to cybersecurity and asset segregation.
- A token mapping exercise is proposed to be undertaken later next year, which would attempt to categorise crypto assets into distinct types, potentially for the purpose of a more varied regulatory regime.

Overview

A proposed licensing regime that would regulate crypto exchanges is being explored, with the Treasury now considering submissions from industry and the public to a Treasury Consultation Paper (TCP).[1] The proposed regime would be similar to the AFSL regime. The TCP was the most recent in a series of ongoing reviews into Australia's payments system, spurred in part by the concern that new service providers within the crypto industry pose significant risks to consumers, following the failure of several crypto exchanges in Australia. The exploration of this new area of law by regulators and legislators also aligns with progress being made in other jurisdictions, notably the EU.

In this article, we discuss the model and alternatives proposed by the consultation paper. In particular, we consider two key implications for the crypto industry: a novel private key custody regime as well as a proposed token mapping exercise to be undertaken later this year.

Proposed scope of CASSPr regulation

The TCP relates to the regulation of CASSPrs, which include crypto exchanges and wallets, as distinguished from initial issuers of crypto assets. This focus on CASSPrs is informed by two foundational principles:

- Regulation according to risk — products and services should be regulated according to risk such that new technologies which reduce risk should be subject to different and lighter regulations.
- Technology neutrality — regulation should "look through" technology, applying standards based on risk so as to foster innovation.

Specifically, the TCP identifies CASSPrs as posing the most significant potential risk to consumers, while crypto assets are currently regulated under consumer and financial product law and, in some cases, may offer increased transparency than their conventional alternatives.

Also notable is the broad definition of a CASSPr — any platform which facilitates exchange, transfer or storage of crypto assets. This new definition, which would capture crypto-compatible payment gateways and digital wallets, is broader than the focus on crypto exchanges by the preceding reports on this topic, including the:

- Review of the Australian Payments System Final Report[2]
- Senate *Select Committee on Australia as a Technology and Financial Centre* Final Report[3] and
- Parliamentary Joint Committee Corporations and Financial Services Report on Mobile Payment and Digital Wallet Services[4]

The broad scope of the CASSPr concept, along with the technology-agnostic principles of the TCP, may introduce unexpected regulatory burden for sectors of the crypto industry that considered themselves distinct from crypto exchanges. One example which is expressly contemplated by the TCP is the possible capture of non-fungible token (NFT) platforms, on the basis that they facilitate exchange of NFTs, which are crypto assets. NFT platforms may not currently have in place

the same level of cybersecurity measures that crypto exchanges do, at least partially due to the relatively recent increase in the value of NFTs.

Proposed model of CASSPr regulation

The TCP proposes a licensing regime for these CASSPrs which would be similar, but separate to, the Australian Financial Services licensing regime. The conditions of each CASSPr's licence would depend on the number and type of services which they offer. The TCP proposes that this licence would carry obligations on CASSPrs to:

- do all things necessary to ensure that:
  - the services covered by the licence are provided efficiently, honestly and fairly and
  - any market for crypto assets is operated in a fair, transparent and orderly manner
- maintain adequate technological and financial resources to provide services and manage risks, including by complying with the custody standards
- have adequate dispute resolution arrangements in place, including internal and external dispute resolution arrangements
- ensure directors and key persons responsible for operations are fit and proper persons are clearly identified
- maintain minimum financial requirements including capital requirements
- comply with client money obligations
- comply with all relevant Australian laws
- take reasonable steps to ensure that the crypto assets it provides access to are "true to label"
- respond in a timely manner to ensure scams are not sold through their platform
- not hawk-specific crypto assets
- be regularly audited by independent auditors
- comply with anti-money laundering and counter-terrorism financing (AML/CTF) provisions and
- maintain adequate custody arrangements

The proposed obligation of all CASSPrs to comply with the Anti-Money Laundering and Counter-Terrorism Financing Act2006 (Cth)[5] (AML/CTF Act) is a major change from current requirements, under which crypto exchanges (and not other types of CASSPrs) are required to simply register with the Australian Transaction Reports and Analysis Centre for AML/CTF purposes. Implementation of this new obligation, including any further developments that may be proposed in the future, may be made difficult by the fact that transactions facilitated by CASSPrs often run on self-executing code and may be designed to preserve anonymity. Developing the AML/CTF framework to accommodate CASSPr compliance may challenge the TCP's stated desire for this legislation to be "technology neutral".

Alternative proposals

The TCP has also proposed two alternative models:

Requiring CASSPrs to hold an AFSL

Under this model, CASSPrs could be brought under the remit of the AFSL by amending s 764A of the Corporations Act 2001 (Cth) to specifically include crypto assets as financial products.

Self-regulation by the crypto asset industry

The crypto industry could develop its own code of conduct. The TCP notes that this approach is similar to that followed in the US and the UK but acknowledges that both jurisdictions are considering additional regulatory obligations for crypto assets beyond the code of conduct.

Key proposal — private key custody regime

Private keys are strings of characters that allow the holder to execute full control over the crypto assets contained in the corresponding wallet. For ease, many crypto exchanges store a user's private keys to a range of underlying wallets, allowing the user to trade a variety of crypto assets while only needing to remember a single password to their account. Private keys are highly sensitive and, if accessed in a cybersecurity breach, may cause significant financial loss.

In addition to the obligations discussed above that would apply to all CASSPrs, the TCP proposes an additional series of obligations that would apply to those CASSPrs which hold private keys to crypto assets on behalf of customers. The proposed regime is modelled to some extent after the existing custodial services regulatory regime and would require CASSPrs to have requisite expertise and infrastructure, implement independently-verified cybersecurity practices and adopt multi-factor (or similar) authentication. It would also create a process for redress and compensation in the event that private keys are lost.

The proposed requirement to ensure consumers' assets are appropriately segregated may have significant impact on some CASSPrs. Many platforms, like investment products, may operate by pooling consumers' assets, consolidating the net orders in a given time period and honouring orders to fund or withdraw from accounts. This may be because CASSPrs lack the technical infrastructure or risk frameworks to execute separate orders

for individual consumers. Such CASSPrs should keep abreast of further legislative developments regarding the segregation obligation resulting from this TCP.

The proposed regime may require significant additional regulation to support the cybersecurity obligations, given the sensitivity of private keys. The existing regime, which has expanded in light of the different forms of custodianship, has demonstrated the need for clear standards in the custodial services industry, particularly regarding the independent verification obligations. If such a regime is implemented, it is likely that there will be an even greater need for articulation of clear standards given the diversity of crypto assets. In this case, CASSPrs should anticipate rules and regulations that may impose significantly more granular obligations than what is contemplated in the TCP.

Key proposal — token mapping exercise

Following the end of the consultation process of the TCP on 27 May 2022, some further developments in the crypto regulatory space can be expected before the end of the year. In addition to a Board of Taxation report on the taxation of digital transactions and assets due by the end of 2022, a token mapping exercise will also be carried out by the Treasury.

This would attempt to "map" crypto assets and the networks they operate on so as to develop a regulatory framework for their regulation, which may involve imposing different obligations on CASSPrs depending on the types of crypto assets they deal with. This would categorise crypto assets into distinct types, such as stablecoins, utility tokens and cryptocurrencies, and would provide relief to the likes of NFT platforms and other platforms which may not pose as large a risk to consumers as, for instance, crypto exchanges. This is the approach taken by the Markets in Crypto-assets (MiCA) Regulation[6] adopted by the European Parliament earlier this year, which also regulates "crypto asset service providers" but which would impose different obligations depending on the type of crypto asset concerned.

However, regulating crypto assets according to type may create regulatory uncertainty amongst industry participants, particularly considering the highly varied nature of crypto assets and the possibility of new classes of crypto assets being developed which cut across categories.

Further, regulating crypto assets according to an official typology may undermine the TCP's stated goal of technological neutrality, imposing obligations and duties based on a summary determination of technology instead of a comprehensive risk analysis. Indeed, crypto assets within the same category may have very different risk profiles for consumers. This was evidenced recently with the collapse of the "UST" cryptocurrency, a stablecoin with an algorithmically — defined mechanism that sought to peg its value to that of the US Dollar. This operates very differently to a stablecoin, which achieves a peg by collateralising its total market cap with actual US Dollars.

It is yet to be seen to what the extent Australian regulation of CASSPrs will be informed by token mapping and whether it will keep in step with the approach taken in the EU. Nevertheless, this exercise may prove to be a useful contribution to increased regulatory certainty for CASSPrs operating in Australia, as well as a more complete regulatory treatment of the entire crypto space.

Conclusion

Crypto exchanges and other CASSPrs are likely to face greater regulation in Australia in the future. At this stage, it remains unclear which exact model will be developed and how broad its reach will be. However, it appears likely that it will share significant similarities with the licensing and custody regime under current financial services legislation.

James North
Practice Group Leader of Technology, Media and Telecommunications
Corrs Chambers Westgarth
james.north@corrs.com.au
www.corrs.com.au

Steven Rice
Partner, Financial Sponsors
Corrs Chambers Westgarth
steven.rice@corrs.com.au
www.corrs.com.au

Lachlan Ellison
Graduate Lawyer
Corrs Chambers Westgarth
lachlan.ellison@corrs.com.au
www.corrs.com.au

Javier Cross
Law Graduate
Corrs Chambers Westgarth
javier.cross@corrs.com.au
www.corrs.com.au

Footnotes

1. The Treasury *Crypto asset secondary service providers: Licensing and custody requirements* Consultation paper (2022) https://treasury.gov.au/sites/default/files/2022-03/c2022-259046.pdf.
2. The Treasury *Payments system review: From system to ecosystem* Final Report (2021).
3. The Senate *Select Committee on Australia as a Technology and Financial Centre* Final Report (2021) https://parlinfo.aph.gov.au/parlInfo/download/committees/reportsen/024747/toc_pdf/Finalreport.pdf.
4. Parliamentary Joint Committee on Corporations and Financial Services *Mobile Payment And Digital Wallet Financial Services* Report (2021) https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024736/toc_pdf/MobilePaymentandDigitalWalletFinancialServices.pdf.
5. Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth).
6. Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937.

Cybercrime — an Australian overview

***Dennis Miralis**, **Lara Khider** and **Mohamed Naleemudeen** NYMAN GIBSON MIRALIS*

Australia has a broad system of federal, state and territory-based laws which govern cybersecurity. This article will discuss the current Australian legislative landscape of cyber laws and future developments and trends as the Australian Government intensifies efforts to introduce legislation that enhances cybersecurity and creates a rigorous framework to combat cybercrime.

Key takeaway points

- Australia has developed an increasingly robust legislative framework to combat cyber-related crimes. A unified legislative approach has been adopted by all levels of government, emphasising the unified focus to combat the evolving typologies of cybercrime.
- In 2021, the Australian Government passed the Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 (Cth) (SLAID Act), which enhanced the ability of the Australian Criminal Intelligence Commission (ACIC) and the Australian Federal Police (AFP) to discover, target, investigate and disrupt serious cybercrime.
- On 15 December 2021, Australia signed the Cloud Act Agreement with the United States of America (USA), which permits the respective governments to obtain information from telecommunication providers in the other country for the purposes of investigating serious crimes.

The federal legislative scheme

In Australia, cybercrime offences broadly encompass two categories:

- offences that are directed at computers or other devices and involve hacking-type activities and
- cyber-enabled offences where such devices are used as a key component of the offence, including in online fraud, online child abuse offences and cyberstalking

On the federal level, the Criminal Code Act 1995 (Cth) (Criminal Code) is the key legislative instrument that criminalises cyber-related conduct. Parts 10.6 and 10.7 of the Schedule to the Criminal Code set out a variety of offences with a range of maximum penalties that range from fines to life imprisonment. The offences include:

- unauthorised modification of data to cause impairment (maximum penalty: 10 years imprisonment)[1]
- dishonestly obtaining or dealing in personal financial information (maximum penalty: 5 years imprisonment)[2]
- creation and distribution of malicious software (viruses, worms, trojans) (maximum penalty: 3 years imprisonment)[3] and
- infection of IT systems with malware (maximum penalty: 2 years imprisonment)[4]

The Criminal Code's cybercrime offences are based on model laws agreed to by Commonwealth, state and territory governments in 2001 under the Cybercrime Bill 2001 (Cth). The purpose of the Bill was to update existing Commonwealth provisions on computer-related crime, including inserting a new Pt 10.7 to the Criminal Code. The offences are consistent with those required by the Convention on Cybercrime, also known as the Budapest Convention, and are drafted in technology-neutral terms to accommodate advances in technology. The Budapest Convention entered into force on 1 July 2004 and was ratified by Australia on 30 November 2012. The Budapest Convention is the first international treaty to provide a legal framework to address internet and computer-related crimes by seeking to align national laws on cybercrime, improve investigative techniques and increase cooperation among countries.

The state legislative scheme

Most states and territories in Australia have codified laws against cybercrime in their respective criminal codes. The state and territory laws are aligned with the Commonwealth cybercrime offences by criminalising the misuse of data and computer systems.

New South Wales (NSW),[5] Victoria,[6] South Australia,[7] Queensland,[8] Tasmania,[9] Western Australia[10] and the Northern Territory (NT)[11] have similar cybercrime and computer-related offences, which include:

- production, dissemination or possession of child abuse material[12]

- filming a person engaged in private act or their private parts, or installing device to film or observe a person[13]
- online fraud[14]
- identity theft[15]
- unauthorised access, modification or impairment of data or electronic communication[16]
- possessing, producing, supplying or obtaining of data with intent to commit serious computer offence[17]
- unauthorised access to or modification of restricted data held in computer (summary offence) and[18]
- unauthorised impairment of data held in computer disk, credit card or other device (summary offence)[19]

Who investigates and/or prosecutes cybercrime in Australia

At the national level, the AFP investigates and responds to cybercrime of national significance. The AFP is also responsible for child protection and investigates crimes associated with online child sex exploitation and travelling child sex offenders.

The AFP is assisted by the Australian Cyber Security Centre (ACSC). In 2017, the Australian Government established the ACSC as a sub-agency of the Australian Signals Directorate (ASD). The ACSC was established to improve cybersecurity, which includes investigating and developing solutions to cybersecurity threats. The ACSC is comprised of staff from the AFP, ASD, ACIC, Department of Home Affairs and Australian Security Intelligence Organisation (ASIO).

The ASD is an Australian Government agency responsible for defending Australia from global threats, foreign signals intelligence and cyber warfare. As an objective of the ASD is to provide advice and assistance to law enforcement, the agency collaborates with federal, state and territory police in relation to matters of national interest.

The ACIC and ASIO, which are members of Australia's National Intelligence Community, also assist in the investigating and analysis of cybercrime and cybersecurity threats. The Australian National Intelligence Community is a collective of agencies that collaborate to collect, analyse and disseminate intelligence information and advise in accordance with Australia's interests and national security priorities.

At the state and territory level, police are responsible for investigating and responding to cybercrime offences. NSW and NT have established specialist taskforces to address cybercrime. In 2017, the NSW police formed "Cybercrime Squad", which is tasked with responding to cyber-enabled and cyber-dependent crimes. The Cybercrime Squad is responsible for investigating complex cyber offences.

The Commonwealth Director of Public Prosecutions (CDPP) pursue criminal prosecutions of offences in breach of Commonwealth cyber laws. State and territory Directors of Public Prosecutions (DPP) pursue prosecutions for cyber offences under state and territory laws.

Recent legislative developments

In 2021, the Australian Government introduced the SLAID Act which amends the Surveillance Devices Act 2004 (Cth) and Telecommunications (Interception and Access) Act 1979 (Cth). This amendment enables law enforcement to obtain "data disruption warrants", which, if issued, permits the AFP and ACIC to intervene in order to disrupt the commission of cybercrime.

At the bilateral level, in December 2021, Australia and the USA entered an Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime (the CLOUD Act Agreement). Once legislated into the respective domestic frameworks, the Agreement will enable law enforcement and national security agencies to issue orders directly to telecommunication providers in the other country for the production of electronic data relevant to investigations or prosecutions of criminal activity. The Agreement is authorised in Australia by the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (Cth) and in the USA by the Clarifying Lawful Overseas Use of Data (CLOUD) Act, a Bill Congress passed in 2018. The CLOUD Act Agreement is undergoing Parliamentary and Congressional review processes in both countries, and if passed, is expected to be enacted in 2022.

Current strategy

The Australian Government published the 2022 National Plan to Combat Cybercrime (the National Plan) on 21 March 2022. The National Plan was an objective of the government's 2020 Cyber Security Strategy.[20] The National Plan builds on the 2013 National Plan to Combat Cybercrime and formalises a framework that focuses on three key pillars:

- prevent and protect
- investigate, disrupt and prosecute and
- recover

The framework aims to support the development of a nationally coordinated approach to combating cybercrime in Australia.

Conclusion

- The Australian Government is moving towards an increasingly robust cybercrime legislative framework, in line with a focused national combat strategy.
- It is expected that the international mutual cooperation between Australia and other countries will continue to advance the way in which countries deal with cybercrime.

Dennis Miralis
Partner, International Criminal Defence Lawyer
Nyman Gibson Miralis
dm@ngm.com.au
https://ngm.com.au/

Lara Khider
Senior Lawyer
Nyman Gibson Miralis
lk@ngm.com.au
https://ngm.com.au/

Mohamed Naleemudeen
Defence Lawyer
Nyman Gibson Miralis
mn@ngm.com.au
https://ngm.com.au/

Footnotes

1. Criminal Code Act 1995 (Cth), s 477.2.
2. Above, s 480.4.
3. Above n 1, s 478.4.
4. Above n 1, s 480.2.
5. Crimes Act 1900 No 40 (NSW).
6. Crimes Act 1958 (Vic).
7. Criminal Law Consolidation Act 1935 (SA).
8. Criminal Code Act 1899 (Qld).
9. Criminal Code Act 1924 (Tas).
10. Criminal Code Act Compilation Act 1913 (WA).
11. Criminal Code Act 1983 (NT).
12. Above n 5, s 91H.
13. Above n 5, ss 91K–91M.
14. Above n 5, s 192E.
15. Above n 5, s 192J–192K.
16. Above n 5, ss 308C–308E.
17. Above n 5, ss 308F–308G.
18. Above n 5, s 308H.
19. Above n 5, s 308I.
20. Department of Home Affairs *Australia's Cyber Security Strategy* (2020) www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.

The Google/Barilaro fiasco!

Patrick George *KENNEDYS*

There has been much debate about the strictness of liability for defamation and the harshness of imposing liability on digital platforms for publishing third party content.

On 6 June 2022, a judgment[1] in the sum of $715,000 was entered against Google LLC, $675,000 in damages (including aggravated damages) and $40,000 interest, for publishing defamatory material uploaded to YouTube by someone else, about the former Deputy Premier of New South Wales, John Barilaro.

One assumes that Google wanted to have a pristine reputation in Australia of being a model corporate citizen. That meant that Google would comply, and be seen to comply, with the law.

Nevertheless, as a digital platform or internet intermediary, and given the law of defamation in Australia, Google would inevitably participate in the publication of defamatory material uploaded to its service by third parties.

As a model corporate citizen, it would only do so unwittingly and without intent to defame, wilful blindness or malice.

It was entitled reasonably to contest its liability, as to whether it participated in the publication of the third party content (at least until the High Court determined otherwise), whether in fact it had knowledge or means of knowledge that the material was defamatory and/or whether it was notified of the defamatory material after first publication, and whether the occasion of publication was privileged by virtue of the legitimate interest of those who downloaded it.

It was reasonable that Google sought to contest these issues in various cases before the courts in Australia. It has been to the High Court twice: *Trkulja v Google LLC*[2] and *Google LLC v Defteros*[3] which awaits judgment.

It faced strict liability for publication of third party content otherwise and large damages awards. The first judgment of concern for Google was in *Trkulja v Google Inc LLC (No 5)*[4] in which the sum of $200,000 was awarded in respect of Google search results of Google images and news.

The next came in *Duffy v Google Inc (No 2)*[5] where $100,000 was awarded in respect of a website "Ripoff" available through Google searches.

More recently, a judgment of $40,000 was awarded in *Defteros v Google LLC*[6] in respect of Google searches providing snippets and links to third party websites.

While such a model corporate citizen would seek to comply with the law as it exists, potential reform would provide some hope for a more reasonable fault-based outcome given the benefits Google provides the public as a global internet service.

Reforms to "modernise" defamation law began to be mooted with momentum in 2018. The first stage was implemented in 2021, with the exception of Western Australia and the Northern Territory, but the reforms did not address protection of digital platforms for third party content.

In March 2021, however, the Attorneys-General for the states and territories issued a Discussion Paper for the Stage 2 Review of the Model Defamation Provisions[7] which specifically concerned the possible relaxation of the strict liability for permitting publication of third party content on digital platforms, possibly even as much as the immunity enjoyed by internet intermediaries in the US.

The Discussion Paper sought to classify internet intermediaries by their functions — "basic internet services", "digital platforms" and "forum administrators" — and postulated immunity for basic internet services, while digital platforms and forum administrators would have express recognition as "secondary" or "subordinate distributors" under the defence of Innocent Dissemination in s 32 of the Defamation Act 2005 (Vic).

This defence recognises the "innocence" of some parties for their subordinate participation in the publication process, such as printers, postal services and booksellers for example. These parties need to show that they were not the author or originator of the matter, that they were not aware that the matter was defamatory, through no fault of their own, and that they had no capacity to exercise editorial control over the content of the matter before it was first published.

In the midst of this debate, in September 2021, the High Court (in *Fairfax Media Publications Pty Ltd v Voller*[8] (*Voller*)) upheld longstanding principles of the law as to publication at common law. It confirmed that forum administrators such as the *Sydney Morning Herald*, *The Australian* and others would be liable for the

publication of third party content (in the absence of defences) where they had facilitated, encouraged and assisted third parties to post material on their websites and platforms. It did not concern whether the innocent dissemination defence applied in the circumstances.

In December 2021, the Commonwealth Government reacted to the High Court decision rushing to legislate the inaptly named "Social Media (Anti Trolling) Bill 2022". Despite its title, its purpose was not to restrain trolling (online abuse, bullying and harassment). Instead, it proposed to provide immunity for forum administrators, such as the media websites publishing third party comments in *Voller*, and a defence for social media providers removing their liability if they complied with a complaints system which enabled identification of the originator or poster of the content.

The Bill lapsed with the Federal election and the new government has no intention of reviving it.

While these steps were taking place, in September and October 2020, Jordan Shanks (known online as "@friendlyjordies") uploaded two videos — "bruz" and "Secret Dictatorship" — to YouTube, a digital platform operated by Google for profit. The videos were found to have formed part of a "relentless, racist, vilificatory, abusive and defamatory campaign" against Mr Barilaro. They imputed he was corrupt; he had committed perjury many times and had engaged in blackmail.

In November 2020, Barilaro's staff asked Google to take down these and other Shanks videos. YouTube had a set of internal policies called "Community Guidelines" which provided a guide of what was not allowed on YouTube. In December 2020, Google declined to remove the videos. On its review of them, it considered that the videos had not violated its Community Guidelines.

Barilaro commenced proceedings for defamation against Shanks and Google. Following a mediation, Shanks settled the claim.

Google did not but continued on with its defences which included:

- a denial that any of the imputations alleged were conveyed
- that they were published under common law Qualified Privilege for those with a legitimate interest, and consistently with the implied freedom under the Constitution
- that they were published under statutory Qualified Privilege as a reasonable publication of information and
- that the "bruz" video was published as an honest expression of opinion by Shanks based on true factual material

Google later amended its claim to assert a defence that Barilaro had consented to edited versions of the videos being uploaded after the settlement with Shanks.

Prior to and up to the first day of the trial, Google progressively abandoned each of these defences.

The statutory cap on damages which applied to the proceedings was $432,500. The cap would not apply however if Google's conduct was found to be "improper, unjustifiable or lacking in bona fides" which aggravated damages.[9]

The Trial Judge (Rares J) found that Google's conduct was improper in failing to remove the videos firstly from the time after complaint was made, from the commencement of the proceedings and finally from the time it acknowledged it did not (and never did) have a bona fide defence.

He said the videos were replete with "racist, hate filled rants that were calculated to bully and publicly hound" Barilaro.[10] He condemned Google's attitude to the merits of the complaint and the claim in the proceedings:

> Hate filled speech and vitriolic, constant public cyberbullying . . . cannot be classified as in any way [an] acceptable means of communication in a democratic society governed by the rule of law. Google's conduct after 22 December 2020 in leaving both Mr Shanks' existing and subsequently posted videos online magnified the hurt to Mr Barilaro's feelings, inflamed hate filled responses directed at him by members of the public in personal confrontations and on social media and allowed a perception, until the trial, that Google actually had a bona fide defence in this proceeding for its conduct.[11]

The Trial Judge proceeded to find that Google had pleaded defences that had no prospect of success, causing Barilaro added distress, damage to his reputation and delay to his vindication. Google encouraged and facilitated Shanks in his vitriolic, obsessional, hate-filled cyberbullying and harassment of Barilaro both before and after Shanks settled the claims against him and it did so with a view to its commercial profit.[12]

Despite multiple breaches of its Community Guidelines governing the use of YouTube and put forward as protecting individuals including public figures from being subjected to racist attacks, harassment, hate speech and cyber bullying, he found that Google chose to continue publishing the material. It did so without acting as a responsible or reasonable publisher.[13]

He referred Google's and Shanks' conduct to the Principal Registrar of the Federal Court to consider whether to institute proceedings for what appeared to be serious contempt of court by bringing improper pressure on Barilaro and his lawyers not to pursue the proceedings.[14]

Google's reputation as a model corporate citizen is in tatters from this fiasco. Worse still, its "innocence" as a

mere internet intermediary has been destroyed by this judgment which will impact on other internet intermediaries as governments, now wary of such claims to innocence, move in the direction of regulating them.

Patrick George
Senior Partner
Kennedys
Patrick.George@kennedyslaw.com
https://kennedyslaw.com/

Footnotes

1. *Barilaro v Google LLC* [2022] FCA 650; BC202205103.
2. *Trkulja v Google LLC* (2017) 263 CLR 149; (2018) 356 ALR 178; [2018] HCA 25; BC201804827.
3. *Google LLC Defteros* [2022] HCATrans 77.
4. *Trkulja v Google Inc LLC (No 5)* [2012] VSC 544; BC201208568.
5. *Duffy v Google Inc (No 2)* [2015] SASC 206; BC201512864.
6. *Defteros v Google LLC* [2020] VSC 219; BC202003565.
7. *Attorneys-General Review of Model Defamation Provisions — Stage 2* Discussion Paper (2021).
8. *Fairfax Media Publications Pty Ltd v Voller* (2021) 392 ALR 540; [2021] HCA 27; BC202108345.
9. Above n 1, at [311].
10. Above n 1, at [324].
11. Above n 1, at [348].
12. Above n 1, at [402].
13. Above n 1, at [404].
14. Above n 1, at [407].

For editorial enquiries and unsolicited article proposals please contact Genevieve Corish at Genevieve.corish@lexisnexis.com.au.
Cite this issue as (2022) 25(2) *INTLB*
SUBSCRIPTION INCLUDES: 10 issues per volume plus binder www.lexisnexis.com.au
SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067
CUSTOMER RELATIONS: 1800 772 772
GENERAL ENQUIRIES: (02) 9422 2222
ISSN 1329-9735 Print Post Approved PP 244371/00049