CAMLA
COMMUNICATIONS AND MEDIA LAW ASSOCIATION

June 2022
Volume 41.2

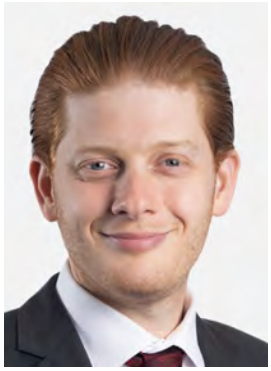
Communications Law Bulletin

Contents

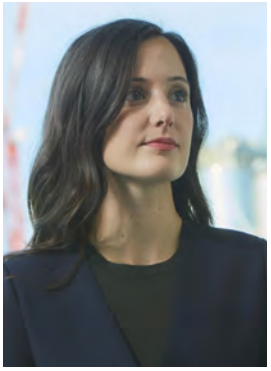
Editors
Ashleigh Fehrenbach and Eli Fisher

Editorial Assistants
Dominic Keenan and Jessica Norgard

Editors' Note



Eli Fisher



Ashleigh Fehrenbach

Our dear CLB readers

We're delighted to present you with our latest edition of the CLB, action packed with content and reports from our events.

Following the previous special International Women's Day edition, which was once again a raging success (if we say so ourselves!), this general edition covers a range of developments from all corners of the CAMLA industries.

There are new laws to discuss, with **Alex Hutchens** (McCullough Robertson) tackling the *Online Safety Act* and **David Kim** (Banki Haddock Fiora) commenting on that law's incursion into defamation territory. **Jamie Wolbers**, **Simone Mitchell** and **Jonathan Kelp** (MinterEllison) write about how the new *Therapeutic Goods Advertising Code 2021* impacts the advertising world, just in time for the 30 June 2022 deadline for ensuring compliance.

There are new cases to discuss, with **Alex Tharby**, **Fabienne Sharbanee** and **Mhairi Stewart** (Bennett + Co) looking at the ***Google LLC v Defteros*** defamation litigation following the 3 May hearing in the High Court. **Georgie Austin**, **Zoe Burchill**, **Blake Pappas** and **Richard Leder** (Corrs Chambers Westgarth) take a look at the first judgment to consider the serious harm test for a defamation action in *Newman v Whittington*. **Alec Christie**, **Avryl Lattin**, **Raeshell Staltare**, **Christian Hofman** and **Alexia Psaltis** (Clyde & Co) take us through *ASIC v RI Advice,* the first case to address whether a failure to manage cyber risk is a breach of a financial services obligations and, possibly, directors' duties. **Marlia Saunders** (Thomson Geer) takes a look at the recent Federal Court decision in *Barilaro v Google LLC* regarding the defamatory videos posted by friendlyjordies. **Helen Macpherson**, **Tanvi Shah** and **Avi Toltzis** (Baker McKenzie) discuss the ***Thaler*** litigation around the world, and the questions it raises about the recognition of AI as an inventor under patent law in various jurisdictions. **Kevin Lynch** and **Jade Tyrrell** (JWS) take us through the Peter Dutton defamation claim, and **Marlia Saunders** and **Jessie Nygh** (Thomson Geer) comment on the Full Federal Court's *Facebook v OAIC* decision.

And there's new law and policy reform being considered, with **Tara Taylor** (McCullough Robertson) tackling the ACCC's fourth interim report, which examines potential competition and consumer issues in Australian general online retail markets. We also hear from **Timothy Webb** (Clayton Utz) on recent developments in the copyright, trade mark, patent and design worlds, as well as some of the key emerging issues in the telecommunications law industry. Tim also shares his expertise and insights on the importance of good communication and creating deep connections throughout your legal career.

We are also pleased to share with you the two top essays from the annual CAMLA Essay Competition. **Adam Lukacs** (University of Queensland) received first prize for his excellent essay on source confidentiality under siege, which discusses how law enforcement powers threaten journalists' ethical obligations. And **Nadine Mattini** (University of Sydney) received second prize for her exquisite essay on the serious harm threshold in defamation cases involving physician review websites. We truly loved both pieces, and are excited for what the future holds for the two authors! Congratulations!

CAMLA has been extremely busy so far this year! We report on seven events that have taken place. There were the three events comprising our **Music Law series**, a seminar updating on **privacy law reform**, our Young Lawyers **Networking Panel Event**, our **Defamation on Digital Platforms** seminar and, of course, our annual **CAMLA Cup**! Many of our seminars can be streamed on demand by members from the CAMLA website, if you were unable to attend at the time.

We're busily preparing our next edition of the CLB, with a special focus on developments in the US. If you would like to contribute, please get in touch.

Enjoy!

Ash and Eli

The CAMLA Board for 2022

President: Rebecca Dunn, Gilbert + Tobin

Vice Presidents
Martyn Taylor, Norton Rose Fulbright
Debra Richards, Netflix

Treasurer: Julie Cheeseman, Bird & Bird

Secretary: Ryan Grant, Baker McKenzie

CLB Editors
Eli Fisher, Paramount Network 10
Ashleigh Fehrenbach, RPC

Committee Members
Sylvia Alcarraz, Dentons
Chris Chow, Creative Lawyers
Gillian Clyde, Beyond International
Jennifer Dean, Johnson Winter & Slattery
Katherine Giles, MinterEllison
Emma Johnsen, Marque Lawyers
Rebecca Lindhout, McCullough Robertson
Marina Olsen, Banki Haddock Fiora
Nicholas Perkins, Ashurst
Marlia Saunders, Thomson Geer
Katherine Sessions, Office of the eSafety Commissioner
Tim Webb, Clayton Utz

CAMLA YOUNG LAWYERS FOR 2022

Chair: Calli Tsipidis, Foxtel
Secretary: Belyndy Rowe, Sainty Law

Committee Members
Anna Glen, ABC
Anna Kretowicz, Judge's Associate
Claire Roberts, 11 Wentworth
Dominic Keenan, Allens
Erin Mifsud, eSafety Commissioner
Imogen Loxton, Ashurst
Isabella Boag-Taylor, Bird & Bird
Jess Millner, MinterEllison
Jessica Norgard, nbn
Justin Kardi, Clayton Utz
Madeleine James, Corrs Chambers Westgarth

A New 'Single Up-to-date' Online Safety Act Regime

Alex Hutchens, Partner, McCullough Robertson, discusses the Online Safety Act coming into effect earlier this year.

Australian end-users and those operating online platforms and services in Australia are now subject to a new and updated online safety regime. The *Online Safety Act 2021* (Cth) aims to provide a single up-to-date safety regime to address pre-existing gaps in legislation and modernise online content schemes.

Amongst notable updates, the Australian Government has created a core set of basic online safety expectations which apply to social media services and other online platforms, reduced content removal response times, updated legislation to clearly capture app distribution services and online search engines by regulation and created a power for the eSafety Commissioner to require Internet Service Providers (**ISPs**) to remove harmful content.

The updates have come into force thanks to the *Online Safety Act 2021* (**Act**) which passed in Parliament on 23 July 2021 and became effective on 23 January 2022. The Act, together with the *Online Safety (Transitional Provisions and Consequential Amendments) Act 2021*, aims to create a fit for purpose regulatory framework for online safety in the digital age.

Core updates

The Act:

a) retains and replicates certain provisions of the *Enhancing Online Safety Act 2015* (Cth) (**EOSA**) that are working well, for example the non-consensual sharing of images scheme;

b) creates and articulates a core set of basic online safety expectations, along with reporting requirements associated with these;

c) replaces the online safety schemes previously contained in schedules 5 and 7 of the *Broadcasting Services Act 1992* (Cth) to address harmful content;

d) creates a new complaints-based, removal notice scheme for cyber-abuse against Australian adults;

e) broadens the cyber-bullying scheme to capture harms occurring on services other than social media services;

f) reduces the timeframe for service providers to respond to removal notices from the eSafety Commissioner from 48 hours to 24 hours;

g) clearly captures app distribution services and internet search engine services in the new online content safety scheme; and

h) establishes a specific and targeted power for the eSafety Commissioner to request or require ISPs to disable access to material depicting, promoting, inciting or instructing abhorrent violent conduct.

Basic online safety expectations and social media services

As part of its investigation into Australia's online safety regime, the Australian Government noted that few online safety requirements existed in legislation for online service providers. The *Enhancing Online Safety Act 2015* (Cth) did contain a number of basic online safety requirements for social media services regarding cyberbullying, however these were limited in scope in terms of the services Australians are using, and on which harmful material is being encountered.

In response, the Australian Government has introduced the concept of 'Basic Online Safety Expectations' (**BOSE**), which will establish a high benchmark for the online services sector to take proactive steps to protect Australians from abusive conduct and harmful content online.

Under the Act, the relevant minister now has the power to make a set of BOSE. Each BOSE will apply to social media services, relevant electronic services or designated internet services, as determined by the Minister.

The Minister will have the power to:

a) prepare and publish a statement on the Commissioner 's website naming and shaming online services who have contravened one or more BOSE for that service. The statement can also list services who have complied with the BOSE; and

b) require a provider of a social media service, designated internet service or relevant electronic service, to prepare and provide reports to the Commissioner about the extent to which that provider has complied with a specified BOSE. A failure to comply with a report request may result in a civil penalty.

Complaints-based, removal notice scheme for cyber-abuse against Australian adults

The Act also establishes a scheme for the removal of cyber-abuse targeted at an adult.

While previous online safety legislation largely aimed to protect children, under the new scheme, social media services, relevant electronic services, designated internet services, hosting services or relevant end-users who posted the abusive material are responsible for taking all reasonable steps to ensure cyber-abuse material is taken down within 24 hours, or a longer timeframe determined by the Commissioner.

Capturing of online search engine providers

Under the new scheme, the Commissioner also has the power to issue a link deletion notice to internet search engine providers, such as Google, to cease providing a link to Class 1 Material within 24 hours.

This is provided that the Commissioner is satisfied that:

- on two or more occasions within the last 12 months end-users could access Class 1 Material using a link provided by that service; and
- during those 12 months the Commissioner had given at least one removal notice in relation to the material that was not complied with.

A failure by a search engine provider to remove a link when requested may result in a civil penalty.

Capturing of app distribution services

Similar to the above, under the new scheme, the Commissioner can also issue an app removal notice to an app distribution service, forcing them to remove the ability for Australians to download infringing apps that facilitate the posting of Class 1 Material within 24 hours.

This is provided that the Commissioner is satisfied that:

- on two or more occasions within the last 12 months Australian end-users could access Class 1 Material by downloading an app provided by that service; and
- during those 12 months the Commissioner had given at least one removal notice in relation to the material that was not complied with.

A failure by an app service provider to block the download of an app by Australian users when requested may result in a civil penalty.

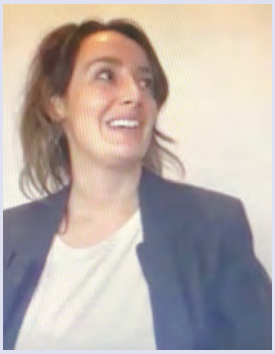
Additional rules for social media and online service providers

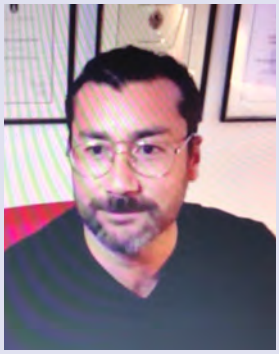
The Commissioner also now has the power to determine additional legislative rules that apply to eight nominated industry groups, including providers of social media services, relevant electronic services, designated internet services, hosting services and internet service providers in relation to each respective service. This includes the power to require industries to develop codes of practice concerned with ensuring the online safety of Australians and addressing the solutions be implemented to achieve the required safety measures.

In exercise of this power, on 11 April 2022 the Commissioner formally notified the six industry associations already developing codes of practice that the codes ought to be ready for registration later this year. If an industry is unable to establish appropriate codes in a timely manner, the Commissioner has the power to declare industry standards.

Event Report: CAMLA Young Lawyers Music Law 101 Seminar

Isabella Boag-Taylor (Bird & Bird, CAMLA Young Lawyers Committee representative)





On 24 March 2022, the CAMLA Young Lawyers Committee (YLC) held its Music Law 101 webinar – the first session in a three-part "Music and the Law" series. The presenters included Chris Chow, Director at Creative Lawyers, Chloe Martin-Nicolle, Director of Legal and Business Affairs at Sony Music Entertainment, and Damian Rinaldi, Principal at Sonic Lawyers. YLC members Jess Millner of MinterEllison and Nicola McLaughlin of NBN moderated the session.

Music law is an incredibly complex area that operates symbiotically with the music industry itself. In many ways, the law has developed along with the industry and many of the legal concepts have arisen as a result of the way the industry is structured. The Music 101 session was an excellent foray into the world of music law by three leading industry experts.

In one short hour Chris, Chloe and Damian covered what it means to be a copyright owner, what rights subsist in musical compositions and recordings, and who owns them. They also discussed the difference between mechanical rights, synchronisation rights, adaptation rights, neighbouring rights, print rights, performing rights, and moral rights, as well as how commercial music, production music, and commissioned music are treated legally. Further topics included a comparison of record labels and music publishers, the key features of music agreements, and the differing legal considerations of new and established artists.

The session was a must-watch in terms of the incredible foundational knowledge imparted by Chris, Chloe and Damian. The key concepts and considerations that were covered were an excellent introduction to, or refresher for, young lawyers or law students interested in or currently practising in music law.

The YLC extends its sincere thanks and congratulations to Chris, Chloe and Damian for a successful webinar.

The session was recorded and is available to members on the CAMLA website.

First Consideration of the 'Serious Harm' Test in Australian Defamation Action

The Supreme Court of New South Wales became the first Australian court to consider the serious harm test for a defamation action in *Newman v Whittington* [2022] NSWSC 249 (**Newman**). **Georgie Austin**, **Zoe Burchill**, **Blake Pappas** and **Richard Leder** (Corrs Chambers Westgath) discuss its implications.

The serious harm test was introduced as part of the Stage 1 Defamation Reforms which came into effect on 1 July 2021.[1] The test requires plaintiffs to establish that a defamatory publication has caused, or is likely to cause, serious harm to their reputation.

The decision in *Newman* confirms that a plaintiff is now obliged to prove serious harm as a fact in every case, abolishing the common law rule which presumed reputational damage upon the publication of defamatory material.

While the serious harm threshold remains undefined, the Court in *Newman* endorsed the UK approach in *Lachaux v Independent Print Limited* (***Lachaux***), which looks to the actual impact of a publication on a plaintiff.

Background

Jasmin Newman, a family dispute resolution practitioner, brought a defamation action against Adam Whittington, an Australian citizen residing overseas.

Newman's claim related to alleged defamatory publications posted online between 29 December 2019 and 21 October 2021. Of the 27 publications, only those published after 1 July 2021 were assessed in accordance with s 10A, the new serious harm provision of the *Defamation Act 2005 (NSW)*.

Among other issues, including proof of publication, the Court considered whether the publications had caused, or were likely to cause, serious harm to Newman's reputation.

Serious harm test

Justice Sackar confirmed that the issue of serious harm would normally be determined before trial unless special circumstances justified its postponement. These circumstances include, but are not limited to, cost implications, the court's resources and whether the determination of serious harm is linked to other issues during the trial.

Justice Sackar considered the UK's equivalent of s 10A in his discussion of how the serious harm test should apply in Australia. Despite minor variations between the two legislative provisions, his Honour observed 'no material difference' between the Australian and UK formulations.

Referring specifically to *Lachaux,* his Honour described the decision as a 'powerful and persuasive analysis' of an analogous provision. While the decision is not binding on Australian courts, Justice Sackar considered it a persuasive authority.

Adopting the reasoning of Lord Sumption in *Lachaux*, Justice Sackar confirmed that a plaintiff must prove serious harm as a necessary element of the cause of action in New South Wales. His Honour also held that s 10A has the effect of abolishing the common law rule that damage can be presumed upon the publication of defamatory statements.

Though not expressly adopted, his Honour also endorsed the UK threshold for serious harm, where harm is determined by reference to the actual facts of a publication's impact, not just to the meaning of the words used.

The decision

In Lachaux, serious harm was established by evidence from the plaintiff and other witnesses. Lord Sumption also considered the scale of the publications and readership figures.

As *Newman* was conducted on the pleadings, no evidence was led as to whether Newman had suffered serious harm. The pleadings asserted that serious harm was to be inferred from the inherent seriousness of the defamatory imputations and from Newman's reputation as a family mediator.

Justice Sacker did not consider that Newman's pleadings clearly articulated an arguable case. However, given the novelty of the point, his Honour granted leave for the plaintiff to replead her claims and demonstrate a valid cause of action.

Implications

Following *Newman*, it appears that *Lachaux* may serve as a template for Australian courts to use when establishing a serious harm threshold. The Court's recognition in Lachaux that the extent of the publication is relevant to seriousness is one approach which may be adopted, either in whole or in part.

For now, this decision places plaintiffs on notice of their positive obligation to prove serious harm as a separate element in a defamation action. It also serves as a reminder of the need to set out the particulars of serious harm at the pleadings stage, as merely asserting serious harm will not be enough.

---

1 *Defamation Act 2005 (*Vic) s 10A.

Profile: Timothy Webb

Timothy Webb, Partner at Clayton Utz, is a leading IP lawyer who advises on both contentious and non-contentious matters. He has a wide range of experience across the spectrum of intellectual property, including copyright, trade marks, patents, designs, advertising, confidential information, domain names and anti-counterfeiting. He has acted for clients in landmark Australian test cases for both copyright and designs, and regularly assists clients in the Copyright Tribunal. Tim is also the joint head of the firm's Trade Mark and Brand Protection Group. Tim is a Fellow of the Chartered Institute of Arbitrators, past member of the Law Society of NSW Litigation Law & Practice and ADR committees, a committee member of the International Trademark Association, and member of the CAMLA Board. Tim's IP expertise is recognised in Chambers, Legal 500, Best Lawyers, Doyle's Guide, Managing IP and World Trademark Review 1000, but he says that is all due to his super talented team. **Ashleigh Fehrenbach,** co-editor, sits down with Tim to discuss his career and insights.

ASHLEIGH: What were two key skills you learnt in your first few years of legal practice?

TIM: I was blessed to work with many fantastically talented lawyers in my first years of practice. The "rotation" system offered by most larger law firms is a wonderful model to expose young lawyers not just to different areas of law and the skills necessary to practise them, but also to different practitioners who have different strengths from which to learn.

The most important skill I picked up is relevant to all areas of the law, and both private practice and in-house. I realised early on the centrality and criticality of communication skills to legal practice. That sounds trite but it is fundamental. So much of what we do – whether drafting transactional documents, preparing advice or advocating a position in court submissions – is about conveying a message that should be clear and achieve an objective. I also learnt early on that much of what makes a communication effective, is its responsiveness. And by "responsiveness" I do not mean "timeliness", but how well it responds to the requirements of the person to whom the communication is being sent. A business might require advice on an issue that could be answered by a 10-page letter replete with case references, or by a two-paragraph email (even if the issues are very complex!). But they are different work products and if one is provided when the other is expected, the only certainty is an unhappy client. So, the skill really is to ask questions to understand the purpose of the communication, and to tailor it accordingly.

Another key skill I learnt, which is a subset of good communication, or might directly feed into subsequent communications, is attention to detail. That can manifest itself in a variety of contexts, for example, remaining focussed while reviewing thousands of discovery documents looking for the "smoking gun" (rarely found!) or a consistent use of active tense and no typos in a simple letter.

ASHLEIGH: You have worked on a range of high-profile IP matters. I'd love to hear about how you found yourself in that specialisation.

TIM: Unintentionally. And there is a good lesson in that too. I started my legal career as a graduate in the Canberra office of Clayton Utz. My first rotation was in the Corporate department (effectively advice and transactions for the Commonwealth Government), then Property, and then in Litigation and Dispute Resolution. A week into that last rotation, I was on a flight to Sydney to meet with Steven Finch SC and Stephen Burley (then a barrister) in chambers to discuss a dispute concerning copyright in the designs of the Collins class submarines. I immediately knew this was what I wanted to do – not just IP, but dispute resolution generally. In 2005 my supervising partner Robert Cutler moved to Sydney and, with my girlfriend (now wife) getting a job in Sydney, we also came up the highway and I joined his team in the Clayton Utz Sydney office. Robert's practice covered both general commercial litigation and IP, so I began doing both types of matters on a regular basis. Having not studied IP as an undergraduate, I did a Master of Laws at UNSW specialising in IP. That study and the wisdom of my colleagues (including Mary Still and John Collins) provided a wonderful platform for me to grow as an IP lawyer.

ASHLEIGH: What do you find most interesting about the world of IP law?

TIM: Its depth, variety and synergy with the modern world economy.

IP law is not homogenous nor simple – each form of IP has its own legislation (in the case of the Copyright Act, now 689 pages!), body of jurisprudence, international framework and law reform agenda. That complexity provides a deep well for intellectual curiosity.

The clients, industries and issues that arise in the practice of IP law are unlimited. Every day is different. In the last couple of days our team has advised a television broadcaster, automotive manufacturer, telecommunications company, media monitoring organisation, railway technology manufacturer, FMCG producer, government department and sporting code operator. Importantly, IP issues arise for businesses of all sizes – from the largest multinationals to the smallest SMEs and individuals. Each grapples with IP issues, and finding solutions to those issues is never repetitive.

Finally, I also love the personalities within the IP legal fraternity. I think it is a perfect size – large enough that you are regularly meeting new people, but small enough that you have repeated dealings with practitioners to develop deep connections.

ASHLEIGH: In private practice, you are no doubt surrounded by the concerns of both rights holders and consumers of creative works. What do you see as being the biggest legal challenge for rights holders in Australia at the moment?

TIM: Australia has an excellent legal system, its IP laws are sophisticated and, while some would disagree with

this, the common law has proven reasonably adept at dealing with novel issues while legislative reform catches up. In my experience, and as a general comment, rights holders are well placed in Australia to develop, protect, commercialise and enforce their IP rights.

I think the biggest legal challenge for rights holders at the moment is what is happening in Russia (if that part of the world is relevant to their business). In response to economic sanctions imposed as a reaction to the Russian-Ukrainian war, Russia has issued decrees effectively legalising infringement of intellectual property owned by individuals or corporations in "unfriendly" countries and by restricting foreign licensors from accessing IP royalty payments. Those "unfriendly" countries include Australia, USA, UK, Canada, Japan, South Korea, New Zealand, Singapore, Switzerland, Norway, Iceland, Taiwan and all 27 members of the European Union. The USPTO has also reported that over fifty bad faith trade mark applications have already been filed in Russia that clearly copy famous brands that have withdrawn from the Russian market, and it will be fascinating to see how these issues will be addressed in the years ahead.

ASHLEIGH: Can you tell us a bit about the key emerging issues in the telecommunications space? How can lawyers who practise in that area keep up with such a constantly evolving industry?

TIM: The telecommunications sector is dynamic. Some of the current hot topics facing the industry include the proposed Telstra-TPG regional network and spectrum sharing deal (with competitors lobbying to have the ACCC oppose the tie-up in its current form), NBN Co's proposed Special Access Undertaking variation which has drawn strong reactions from the ACCC and retail service providers, the sale and restructuring of mobile tower assets, expansion of the consumer data right to the sector, the so-called "scissor effect" of a widening gap between revenue and network expenditure, and the repositioning of the telco value proposition including as IP content licensors.

I find the best way to keep abreast of developments is to read industry publications (such as Communications Day and, of course, the Communications Law Bulletin), follow the activities of the players in the industry (including Communications Alliance), work on matters, and have inquiring conversations with those who contribute to the telco sector. And of course attend relevant CAMLA seminars!

ASHLEIGH: What is one development in the IP legal landscape that you are keeping your eye on this year?

TIM: I am keeping my eye on a few things; perhaps I can mention one for each of the most prominent forms of IP.

In copyright law, consultation on the exposure draft of the Copyright Amendment (Access Reforms) Bill 2021 closed earlier this year. I understand that the Department of Infrastructure, Transport, Regional Development and Communications received a lot of feedback, some stridently expressed, so it will be very interesting to see whether those reforms are progressed, and in what form.

The Trade Marks Office is concerned to ensure quality and consistency in the examination of trade marks. It has issued a position paper on how best to assess distinctiveness of marks under application in the light of the High Court decision in Cantarella, including principles relating to the examination of descriptive marks or having a geographical reference but which are not 'geographical indications'. My colleague Brett Doyle is the delegate to the Trade Marks & Designs Consultation Group for the International Trademark Association, and has made an erudite submission on these issues. I will be keenly looking out for any revisions to the Trade Marks Manual of Practice and Procedure.

In the patent space, in April an enlarged five-judge bench of the Full Court of the Federal Court overturned a previous landmark decision in which Beach J found that artificial intelligence (AI) is capable of being legally recognised as an "inventor", as is reported elsewhere in this edition. The outcome of Dr Thaler's special leave application to the High Court will be interesting. I will also be awaiting the High Court's decision in the Aristocrat matter, which was heard in June, which relates to the patentability of computer implemented inventions.

Finally, for designs, reforms from the Designs Amendment (Advisory Council on Intellectual Property Response) Act 2021 came into effect earlier this year, and I will be fascinated to see whether introduction of a grace period and simplification of the designs registration process encourage more designers to file applications.

ASHLEIGH: What is one piece of advice you would share with a young lawyer in the early stages of their career?

TIM: At the risk of making it a theme, I am going to provide more than one, as good advice should be shared and I don't get a platform like this every day!

Enthusiasm to do a task can leave an impression on others as important as how the task is performed. View all work product from the client's perspective, and what will make the job they have to do easier. Invest in developing professional relationships with as many people as time permits. Don't be too anxious about stressful things, or hard on yourself for any mistakes – this is a helpful lens to calibrate: if no one will remember it 2 years from now, it isn't that important. Be open to different paths, appreciating that setbacks can be positives and positives can be setbacks – there is a lot of wisdom in Alan Watts' Story of the Chinese Farmer (check it out on YouTube). Most importantly, a legal career is just one part of life, and always keep your primary relationships strong.

ASHLEIGH: Finally, what do you think of CAMLA's new logo?

TIM: As a trade mark lawyer, I think it is distinctive. As a CAMLA board member, I am grateful for the hard work of those involved in developing it. As a punter, I think it looks pretty good. So overall two thumbs up!

Ashleigh Fehrenbach

The High Court Considers: Does Google Search Publish Every Website on the Internet? Looking Forward to *Google LLC v Defteros*

Alex Tharby, Fabienne Sharbanee and **Mhairi Stewart,** media lawyers at Bennett + Co, consider the Google LLC v Defteros defamation litigation.

Although many are slow to admit it, most of us have succumbed to the urge to type our own names into Google. For some, the search results link to defamatory third-party websites. Should Google be liable for those websites' content when it merely hyperlinks those websites in its results? This is the question the High Court is considering in the *Google v Defteros* appeal after Google was held liable for such content at first instance and on appeal.

This article traces the case history and the submissions made by the parties, and predicts the outcome of the High Court appeal that was argued before the full bench of the High Court on 3 May 2022.

Procedural history

In 2016 Victorian criminal lawyer George Defteros commenced defamation proceedings against US behemoth Google. Online searches for Mr Defteros' name produced a page of results which included links to news articles which defamed him. Google failed to remove the links after Mr Defteros complained of them. The hyperlinks were eventually removed from search results during the course of the proceedings.

Mr Defteros' argument that Google is liable for those links was accepted by the Victorian Supreme Court and Court of Appeal, which also rejected defences of innocent dissemination and common law qualified privilege.

At first instance: *Defteros v Google LLC* [2020] VSC 219[1]

The trial judge, Richards J, held that Google could be liable as a 'publisher' of defamatory matter by the inclusion in search results of hyperlinks to websites that were defamatory. Her Honour followed the seminal case of *Webb v Bloch* (1928) 41 CLR 331 in which Isaacs J held that any degree of participation in the publication of defamatory matter was sufficient to attract liability as a publisher. This case was recently affirmed by the High Court in *Voller* (which was published after the first instance and appeal decisions in the *Defteros* matter).[2] Her Honour found (at [55]) that:

> The inclusion of a hyperlink within a search result naturally invites the user to click on the link in order to reach the webpage referenced by the search result … the provision of a hyperlink within a search result facilitates the communication of the contents of the linked webpage to such a substantial degree that it amounts to publication of the webpage.

Thus by presenting a hyperlink within search results, Google had participated in the publication of its content to the user.

Google also raised defences of innocent dissemination and common law qualified privilege. Google relied on inaccuracies (and apparent falsities) in Mr Defteros' notifications of the defamatory websites to assert that his notifications were insufficient to impute 'knowledge' of them. Richards J rejected this submission and held that the defamatory websites were sufficiently identifiable for Google to have identified them and removed the hyperlinks from search results. The evidence established that Google could have removed hyperlinks to defamatory websites within 7 days, so Google was liable thereafter.

Richards J considered the relevant authorities relating to common law qualified privilege and concluded that although Google provides a service to its users it does not do so as a matter of legal, social or moral duty but as a result of its commercial interests. Her Honour noted that Google's search engine process was fully automated and did not limit its provision of hyperlinks to persons who had a legitimate duty or interest in the search results. Her Honour considered that a user entering a search query and Google presenting search results in response did not necessarily establish a relationship involving a community or reciprocity of interest between the user and Google.

However, her Honour largely upheld Google's defence of statutory qualified privilege. Her Honour inferred that most but not all of the 150 search engine users who 'clicked through' to the defamatory website would have had some interest in the search results, such as seeking Mr Defteros' contact details or services as a lawyer or employment with his firm.

Richards J awarded $40,000 damages to Mr Defteros.

The Court of Appeal's decision: *Defteros v Google LLC* [2021] VSCA 167[3]

The Victorian Court of Appeal (Beach, Kaye and Niall JJA) upheld Richards J's decision on appeal. The Court placed emphasis on the decision in another case involving Google,

1 See our detailed review of the first instance decision: Michael Douglas, Alex Tharby and Jessica Border, 'Google as publisher of everything defamatory on the internet: Defteros v Google LLC [2020] VSC 219', *Bennett + Co* (online) (7 May 2020) < https://bennettandco.com.au/areas/defamation/google-as-publisher-of-everything-defamatory-on-the-internet-defteros-v-google-llc-2020-vsc-219/>.

2 *Fairfax Media Publications Pty Ltd v Voller* (2021) 95 ALJR 767.

3 See our detailed review of the Court of Appeal's decision: Alex Tharby, 'Google Liable in Defamation for Links to Defamatory Websites: Defteros v Google LLC [2021] VSCA 167', *Bennett + Co* (online) (13 May 2020) <https://bennettandco.com.au/areas/defamation/google-liable-in-defamation-for-links-to-defamatory-websites-defteros-v-google-llc-2021-vsca-167/>.

Google Inc v Duffy (2017) 129 SASR 304. That case involved 'snippets' generated by Google that provide a snapshot, or snippet, of part of the hyperlinked website which snippets were themselves defamatory. The Court of Appeal explained the result in *Duffy* in the following terms (at [87]):

> The concepts of incorporation by Kourakis CJ and enticement by Hinton J [ie, the Judge at first instance in *Duffy*] are used to explain why Google was a publisher of material that is linked by means of a URL contained within a search result. They are both a manifestation of the more broadly expressed test in *Webb v Bloch* that fastens on steps that lend assistance to the publication. Here, both concepts can be applied ... The combination of the search terms, the text of the search result and the insertion of the URL link filtered the mass of material on the internet and both directed and encouraged the reader to click on the link for further information.

The Court of Appeal applied the principles from *Webb v Bloch* and *Duffy* and held Google was liable as a publisher of the websites, despite the hyperlinks not themselves being defamatory.

The Court of Appeal upheld Richards J's reasoning and findings in relation to innocent dissemination and the effectiveness of Mr Defteros' notifications and, in effect, in relation to common law qualified privilege. The Court of Appeal also rejected an appeal by Mr Defteros in relation to other matters.

Issues for the High Court to consider

The four issues before the High Court are:

1. whether, by providing a hyperlink to a defamatory third party website in search results, Google is a 'publisher' – in the technical defamation law sense of the content of the third party website;

2. for the purposes of the common law qualified privilege defence, whether Google and all search engine users have a reciprocal duty or interest in relation to search results;

3. for the purposes of the statutory qualified privilege defence, whether all search engine users have 'an apparent interest' in search results by reason of having entered search terms that generated those results; and

4. what is effective notification to a publisher for the purposes of the defence of innocent dissemination?

Analysis of Google's arguments in the High Court[4]

Publication

Google relied on the Canadian Supreme Court decision in *Crookes v Newton* [2011] 3 SCR 269 to submit that the provision of a 'mere collection of mere references' that themselves were devoid of any defamatory content is insufficient to render a defendant a publisher of the website's content. Counsel for Google drew an analogy between search engine operators and a supplier of motor vehicles which carry newspapers with defamatory content in support of Google's position.

Mr Defteros submitted that, on the facts of the case the application of the *Webb v Bloch* and *Voller* tests of any degree of participation in the process of publication, Google should be held liable.

The High Court in *Voller* has already confirmed that "the publication rule has always been understood to have a very wide operation".[5] It is therefore difficult to see Google's appeal on this issue succeeding. During submissions, Kiefel CJ noted that the High Court in *Voller* did not adopt any of the reasoning in *Crookes v Newton*, and Gordon and Gageler JJ each pushed back on Google's submissions. Google's argument might, however, enjoy some support from Edelman and Steward JJ, both of whom engaged with Google's analogy and delivered dissenting judgments in *Voller*.

Common law qualified privilege

Google submitted that a "search engine provides an indispensable means by which users can locate information of interest to them on the internet" and therefore operated for the common convenience and welfare of society. Accordingly, search engine operators have a duty or interest to publish search results and because, as Richards J found, the majority of users use search engines for legitimate interests, the common law should protect search engine operators in respect of publication of results to *all* users.

Mr Defteros submitted that Google's search algorithms were fully automated to return results, whether or not relevant to the user's purposes (whatever those purposes might be), and further, that Richards J had found as a fact that some users accessed the article out of idle interest or curiosity.

The conclusion called for by Google would delineate a new category of qualified privilege between search engine operators and users. Google's submission to the effect that it provides a public service is somewhat undermined by the fact that it operates for profit with its own terms of use. If Google's argument in this regard were affirmed, it would afford search engine operators a defence regardless of the intention of the user and regardless of the content of the search results.

In our view, the High Court is highly unlikely to extend common law qualified privilege this far. The Court might go so far as to afford protection at common law to search engine operators where the user has a recognisable duty or interest in the results, but not otherwise.

Statutory qualified privilege

Google submitted that in addition to the 'interest' it had in publishing search results, it had an 'apparent interest' because its representative reasonably believed that users searching for Mr Defteros' name had an apparent interest in the search results.

Mr Defteros responded that because of the automated nature of the search results that were typically impossible to predict, Google could not have had a reasonable belief that users had an apparent interest in the results.

---

4 *Google LLC v Defteros* [2022] HCATrans 77.

5 *Voller* [31] (Kiefel CJ, Keane and Gordon JJ) and see [88]–[89] (Gageler and Gordon JJ).

The difficulty with Google's submission is one of timing. At the time of the search results' publication – that is, when the search engine user clicks the hyperlink and comprehends the defamatory website – Google has not (and could not have) considered the interests of the *particular* user. It cannot therefore hold the relevant belief at the time of publication. For this reason, it is difficult to see the High Court concluding that Google's blanket belief, that all users searching Mr Defteros' name had an apparent interest in the search results, was reasonable.

Innocent dissemination

Google submitted that: (i) Mr Defteros' notifications contained 'materially' or 'egregiously' misleading statements; (ii) the function and purpose of the innocent dissemination defence is to permit a publisher time to consider its position and response; and (iii) a defendant should not be burdened with having to consider the defamation unless the notice is 'sufficiently square and proper'.

Mr Defteros responded that the notifications included the relevant website addresses and so were sufficient for Google to have identified the material the subject of the complaint.

In our view, Google's submission in this regard ignores the fact that it was provided with sufficient information to identify and remove the hyperlinks from its search results.

The initial "removal request" made through Google's standard process identified the offending URLs. It was only in responding to subsequent requests for further information that Mr Defteros' representatives provided inaccurate information. Nothing in the defence deprives a plaintiff of a cause of action or remedy on the basis that its notification contained inaccuracies, no matter how significant or whether deliberate or not, if the defamatory material has been brought to the defendant's notice.

Prediction

We expect that the appeal will be dismissed in a majority decision that will reaffirm the strictness of 'publication' in defamation law that was affirmed in *Voller*. Unless members of the Court develop the law, Google's prospects of success on its defences are also, in our view, marginal.

Such a decision may re-agitate calls for law reform in the vein of the lapsed and misleadingly-titled *Anti-Trolling Bill*, which has been convincingly derided in many different publications.

From our perspective, Google enjoys sufficient protection with the innocent dissemination defence and under the *Online Safety Act 2021* (Cth). Our current law strikes a fair balance between Google's commercial interests, the public's interest in having access to information, and individuals' interests in seeing their reputations protected.

Event Report: International Privacy and Data Developments with Bird & Bird

Anna Kretowicz (CAMLA Young Lawyers Committee representative)

Privacy. We all want it, especially in a world where data leaks and hacking seem to be happening with increasing frequency, and you think your phone is listening to you because you mentioned to your friend one time that you wanted an Oodie and now your Facebook feed is covered in ads for them. And not to mention the looming spectre of artificial intelligence.

The seminar was held remotely on the evening of 31 March by **Bird & Bird**, with an expert panel of Francine Cunningham (Regulatory and Public Affairs Director), Alex Dixie (Partner and Head of AdTech Practice), Sophie Dawson (Partner), Joel Parsons (Senior Associate) and Emma Croft (Associate). Attendees were given a global view of the trends, developments and forecasts in data and privacy law, with a special focus on the European Union and United Kingdom and how that landscape compares to Australia.

At a high level, the key trends in privacy and data were identified as increasing regulation, giving consumers more control, and cyber security. These changes will have implications across the technology, media and telecom (TMT) environment, affecting businesses, how media is delivered and how journalists can conduct their work.

Summarising the EU position, Francine identified the "Big 5" pieces of legislation in relation to data and privacy that, together, demonstrate a shift towards a "Data Access By Design" model. That is, there's a focus on mandating data portability, making data accessible to users and opening up the market to smaller players in business. Alex added that there is increasing regulation and enforcement of cookies in the UK, which is a predominantly political movement driven by privacy activism, high-profile regulatory decisions and key regulatory opinions.

Turning to Australia, Joel and Emma focussed on the *Privacy Legislation Amendment (Enhancing Online Safety and Other Measures) Bill 2022,* or the OP Bill, which is a direct response to findings made by the Australian Competition and Consumer Commission's Digital Platforms Inquiry in its Final Report of June 2019. Within that, the Online Privacy Code was identified as the key reform to watch out for, which will establish a code of conduct in relation to privacy practices of online platforms.

Privacy law reform doesn't stop there, though, with longer-term changes being explored in the *Privacy Act Review: Discussion Paper,* submissions for which closed earlier this year. That paper explores bigger picture reforms, like changes to the definition of "personal information", the journalism exemption and individual rights like a statutory tort of privacy.

When asked what the future holds, Sophie wrapped up the seminar by saying that it will be important to map and understand data and data practices, be ready for privacy and data portability changes, and generally, to stay abreast of the ever-changing legislative landscape and what it requires.

On behalf of CAMLA, the CAMLA Young Lawyers Committee would like to extend its thanks to Bird & Bird for hosting and leading the discussion with such a knowledgeable and engaging panel, and would like to acknowledge and thank Julie Cheeseman and James Hoy for their work in preparing the seminar.

Massive Defamation Payout Awarded Over YouTube Videos – Will Google Appeal?

Marlia Saunders, Partner, Thomson Geer summarises the recent Federal Court decision in *Barilaro v Google LLC [2022] FCA 650* (6 June 2022).

Google has been ordered to pay $715,000 in damages and interest to former deputy Premier of NSW, John Barilaro, following his successful defamation action over two videos published on YouTube by 'friendlyjordies'.

On 6 June 2022, Justice Rares of the Federal Court of Australia delivered his findings that Google had "encouraged and facilitated Mr Shanks in his vitriolic, obsessional, hate filled cyberbullying and harassment of Mr Barilaro" and, in failing to take down the videos, had aggravated Mr Barilaro's damage such as to warrant a significant award of $675,000 in damages and $40,000 in interest.

The trial in these proceedings was limited to an assessment of damages after Google withdrew its defences, and does not create any new law apart from a non-binding finding by the judge that the new public interest defence in s 29A of the *Defamation Act 2005* (NSW) (**Defamation Act**) can only apply to online publications which were first uploaded on or after 1 July 2021.

However, the decision is significant because it is the first Australian defamation judgment against Google in relation to YouTube content and imposes inordinate responsibility on a secondary publisher for content it did not create, endorse or authorise. It will be interesting to see whether Google appeals, particularly in relation to the Court's finding that Google was liable for damage that accrued prior to it becoming a publisher of the content.

Background

Mr Barilaro claimed that two YouTube videos posted by friendlyjordies falsely conveyed imputations that he is corrupt, committed perjury and engaged in blackmail. In the videos, friendlyjordies parodied Mr Barilaro's Italian heritage and accent, comparing him to Super Mario Brothers, the mafia and a meatball, and calling him offensive and racially-charged names.

Mr Barilaro initially raised concerns about 11 friendlyjordies videos with Google Australia's public policy and government relations team, which escalated them to Google's "Trust and Safety Team" in the US. Google has a set of internal policies, called 'Community Guidelines' which outline the types of content which are not acceptable on YouTube, including vulgar language, harassment, cyber-bullying and hate speech. Google determined that none of the 11 videos violated their policies. Two weeks later, Google advised friendlyjordies that it had taken down one video and advised Mr Barilaro that it declined to take any action in relation to the remaining videos.

It was agreed between the parties that Google became liable as a publisher of the videos when it received a concerns notice from Mr Barilaro's lawyer on 22 December 2020. As a result, there is no discussion in the judgment about the innocent dissemination defence under s 32 of the Defamation Act, which provides that a subordinate distributor is not liable in defamation if they neither knew, nor ought reasonably to have known, that material was defamatory.

Defences

Proceedings were commenced in the Federal Court of Australia on 27 May 2021 against both the creator of friendlyjordies, Jordan Shanks-Markova, and Google in relation to just two of the videos. In July 2021, Justice Rares granted Barilaro leave to serve Google in the United States.

In the meantime, Mr Shanks was required to file his defence. He initially pleaded defences of truth, contextual truth, honest opinion and qualified privilege. Justice Rares held in an interlocutory judgment that Shanks could not, due to parliamentary privilege, plead truth to imputations that Mr Barilaro perjured himself in giving evidence to a committee of the Legislative Council of NSW because Article 9 of the *Bill of Rights 1688 (Eng)*, which applies to proceedings in all Australian parliaments, prohibits anyone impeaching or questioning in any court, the freedom of speech, debates or proceedings in Parliament, including any Parliamentary committee.

Google then filed its defence, pleading qualified privilege, honest opinion of a commentator and the newly introduced public interest defence in respect of publications of the videos which occurred after the defence came into effect on 1 July 2021.

Mediation

Following a mediation in October 2021, Mr Barilaro settled with Mr Shanks, with Mr Barilaro discontinuing the proceedings against him in exchange for payment of $100,000 towards his costs. In the terms of settlement, Mr Shanks agreed to edit the two videos sued on to remove certain portions which conveyed the defamatory imputations. Google sought to argue that Mr Barilaro had consented to the publication of the edited videos. Mr Barilaro denied this and said that Google's conduct in leaving up the edited videos aggravated the damage done to him.

Damages

In the weeks prior to the trial commencing, Google notified Mr Barilaro that it was withdrawing its defences other than the public interest defence. On the first day of trial, after Mr Barilaro's senior counsel stated that he was not making any claim for publication after 1 July 2021, Google notified that it would not press its public interest defence. The trial was therefore limited to an assessment of damages.

Compensatory damages

Google argued that it was not liable for any harm that Mr Barilaro suffered in the period prior to it becoming liable as a publisher on 22 December 2020. It was contended the damages

should be reduced significantly since most of the harm to Mr Barilaro caused by the videos would have occurred shortly after they were uploaded in September and October 2020, when the number of views would have been at their highest.

However, Justice Rares held at [284]: "*A publisher cannot lead evidence of similar or earlier publications for the purpose of establishing that the publisher's defamatory publication did not cause all of the damage of which the claimant complains in a proceeding for defamation*." His Honour said at [288]: "*Mr Barilaro should not have his damages discounted on Google's erroneous hypothesis that by the time it had notice of the defamatory character of those videos, namely 22 December 2020, Mr Barilaro's reputation had already been tarnished and his feelings hurt so that it only had to compensate him for any further damage to his reputation or feelings*." This finding was reached despite his Honour having recognised in a previous interlocutory judgment that Mr Barilaro only sought to rely on publication by Google that occurred after 22 December 2020.[1]

Further to this, Mr Barilaro did not claim any damages after 1 July 2021. This was the stated reason why Google withdrew its public interest defence. Despite this, Justice Rares appears to have counted the number of views during the period between 1 July 2021 and November 2021 (when Mr Shanks edited the videos) in conducting his damages assessment.

Aggravated damages

In support of his claim for aggravated damages, Mr Barilaro sought to rely on Google's failure to take down the videos, Google's conduct of the proceeding and Google's failure to apologise.

In relation to Google's failure to take down the videos, Justice Rares found that Google should have found that the videos breached its policies. His Honour said Google "*operates a very large business in Australia, has Australian staff and lawyers and could not suggest that it was somehow ignorant of how hurtful and bullying the bruz video was in its use of the slurs and venomous hate speech that Mr Shanks directed avowedly, deliberately at Mr Barilaro*".

Justice Rares found the continued publication of other friendlyjordies videos which had not been sued on was also aggravating. His Honour said: "*those videos compounded the harm to Mr Barilaro's reputation from the matters complained of and provoked numerous comments from the public so that they can be taken into account without a discount even if they were online before 22 December 2020, including because Google left them there afterwards*". Justice Rares also found that Google had no reasonable basis to continue to publish the edited versions of the matters complained of, despite Google's argument that Mr Barilaro had consented to their publication in his settlement with Mr Shanks.

While Google asserted that it was critical to distinguish Google's position from that of Mr Shanks because it was "not the creator of the content", Justice Rares rejected this as untenable, stating: "*Google made a deliberate decision on 22 December 2020 to publish the matters complained of and other videos then online and, in doing so, became fully liable as a publisher, including for Mr Shanks' state of mind*." It was therefore held that Google's initial inaction from late December 2020 and its subsequent continuing failure to remove the matters complained of and other videos in Shanks' "ongoing campaign of harassment and abuse" aggravated the damages very substantially.

Justice Rares also found that Google's maintenance of "untenable" issues, such as its denial that the imputations were conveyed and its pleading of defences that it later withdrew, was aggravating. His Honour observed that the qualified privilege defence was hopeless because Google "*made no attempt to seek, let alone put, Mr Barilaro's side of the various subjects on which he was attacked*" and that the honest opinion defence was hopeless because of the "*many misstatements and distortions*" in the videos. In so finding, Justice Rares appears to have imposed journalistic standards on Google, despite the fact that it is not a primary publisher.

His Honour also found the public interest defence was hopeless because s 29A of the Defamation Act, which took effect from 1 July 2021, only provides a defence in relation to electronic defamatory matter which is first uploaded on or after 1 July 2021 due to the operation of the transitional provisions in the Defamation Act and the *Limitation Act 1969* (NSW). In any event, Justice Rares also found it impossible to discern how Google could have believed that continued publication of the videos was reasonable in the public interest given their content.

Justice Rares found that Google's failure to apologise aggravated the damages substantially.

Assessment of damages

In assessing the damages to be awarded, Justice Rares found that Google assisted Mr Shanks to "disseminate his poison" in order to earn revenue under its business model, and in doing so, acted without regard to being a responsible or reasonable publisher.

Overall, Justice Rares stated at [405]: "*Having regard to all of the evidence, the gravity of the imputations, the harm to Mr Barilaro's feelings and reputation, Google's significant aggravation of the damage and the need to vindicate Mr Barilaro's reputation, I consider that he is entitled to judgment in the sum of $675,000. He is also entitled to prejudgment interest from 22 December 2020 of $40,000*."

Contempt referral

After proceedings had been foreshadowed, and again once proceedings had commenced, Mr Shanks continued to post further videos which denigrated Mr Barilaro for commencing the proceedings and also criticised Mr Barilaro's lawyers. Justice Rares held in his judgment that the videos "*were brazen attempts to bring improper pressure to bear on each of them*". His Honour referred the conduct of both Shanks and Google to the Principal Registrar of the Court to consider whether to institute proceedings for contempt of Court.

Next Steps

The parties will now be required to make submissions on costs. Justice Rares essentially invited Mr Barilaro to make an application for indemnity costs.

It appears Google also has a number of arguable appeal points which, if upheld, may result in the quantum of damages awarded being substantially reduced. In particular, the finding that Google was liable for damage caused to Mr Barilaro before the date on which it became liable as a publisher under the law of defamation seems particularly problematic, and should be clarified.

1 *Barilaro v Shanks-Markovina (No 3)* [2021] FCA 1100 (31 August 2021)

A New 'Marker' for Cyber Security Practices
Implications of the RI Advice Group Decision

Alec Christie (Partner), **Avryl Lattin** (Partner), **Raeshell Staltare** (Special Counsel), **Christian Hofman** (Associate), **Alexia Psaltis** (Associate), Clyde & Co, comment on ASIC v RI Advice, the first case to address whether failing to manage cyber risk is a breach of financial services obligations and, possibly, directors' duties.

Introduction

On 5 May 2022, the Federal Court of Australia delivered its judgment in *Australian Securities and Investments Commission v RI Advice Group Pty Ltd* (***ASIC v RI Advice***) – the first case dealing with the issue as to whether failure to manage cyber risk is a breach of financial services obligations.

The Court made declarations that RI Advice Group Pty Ltd (**RI Advice**) had contravened its obligations as the holder of an Australian Financial Services Licence (**AFSL**) holder under sections 912A(1)(a) and (h) of the *Corporations Act 2001* (Cth) (**Corporations Act**) by failing to have appropriate cybersecurity controls and cyber resilience in place to manage its own cyber risks, and cyber risks across its network of authorised representatives (**ARs**).

Importantly, the Court emphasised that while there is a community expectation that reasonable cybersecurity measures are in place, the adequacy of cyber risk management must be determined by technical experts.

While the case focussed on the obligations of RI Advice as an AFSL holder, it nevertheless provides good general guidance for non-AFSL holders and directors of all companies as to how to best manage their own cyber risks to an acceptable standard

Background

ASIC v RI Advice was the first case brought by ASIC alleging that a failure to adequately manage cybersecurity risk is a breach by an AFSL holder of its core financial services obligations.

Although the matter was set down for trial in April 2022, RI Advice admitted a number of contraventions and the matter settled with the parties proposing declarations and orders to be made by consent with an agreed statement of facts (**SAFA**). Both parties filed submissions in support of the proposed declarations and orders.

Having considered the SAFA and the parties' submissions, Justice Rofe of the Federal Court considered there to be a proper basis for making the proposed declarations and orders in the form agreed by ASIC and RI Advice. In her Honour's reasons for judgment, she set out how AFSL holders should manage cyber risk. However, as we have noted, we believe that these reasons could equally apply to non-AFSL holders (in particular, company directors).

Key Takeaways from *ASIC v RI Advice*

- Cyber risk management is a highly technical area of expertise.
- The assessment of the adequacy of any particular cyber risk management systems requires the technical expertise of a relevantly skilled person.
- While there is an element of public expectation in the cyber standard, the relevant standard for the line management of cyber risk and associated controlled measures is not to be determined by reference to public expectation. It must be proportionate to the specific cyber risks facing the AFSL holder and its ARs as determined by technical experts. It could be inferred that the same might apply to non-AFSL holders, especially directors as regards the performance of their directors' duties particularly in relation to their company's cyber security generally.
- In the context of cyber risk management, the assessment of "adequate risk management systems" requires consideration of the risks faced by a business in respect of its operations and IT environment.
- It is not possible to reduce cybersecurity risk to zero, but it is possible to materially reduce cybersecurity risk through adequate cybersecurity documentation and controls to an acceptable level.
- Where cyber incidents occur, it is important that initiatives are taken quickly to improve cybersecurity and cyber resilience. Failure to implement necessary measures in a timely manner can constitute a breach of financial services obligations, or other more general obligations for non-AFSL holders (e.g. directors duties around cyber security).
- This case is the culmination of ASIC's focus on cybersecurity over the last 18-24 months. The emphasis on building cyber resilience is also in line with developments in other regulated sectors and the requirements foreshadowed by the critical infrastructure changes late last year and early this year.

Conduct of RI Advice

RI Advice is the holder of an AFSL under the Corporations Act. In turn, RI Advice also authorises and engages independent owned corporate and individual ARs to provide financial services to retail clients on RI Advice's behalf under its AFSL.

Between June 2014 and May 2020, various ARs of RI Advice experienced nine cybersecurity incidents.

Inquiries and reports made on behalf of RI Advice following the AR cyber security incidents revealed that there were a variety of concerns as regard the ARs' management of cyber security risks.

Admissions by RI Advice

In reaching a settlement with ASIC, RI Advice admitted that, prior to 15 May 2018, it did not have "adequate" cyber risk management systems (including documentation, controls and assurance) to manage cybersecurity risks across its ARs.

Although RI Advice made some significant improvements to its cybersecurity risk management systems including adopting a Cyber Resilience Initiative, RI Advice also admitted there should have had been a more robust implementation of cyber resilience prior to August 2021. It admitted that it "took too long to implement and ensure such measures were in place across its AR practices".

Overview of the decision

What is cybersecurity?

In the circumstances of RI Advice's financial services business, the Court defined cybersecurity as *"the ability of an organisation to protect and defend the use of cyberspace from attacks"* and cyber resilience as *"the ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises on systems that use or are enabled by cyber sources."*

What is adequate cyber risk management?

While the Court did not go so far as to define specifically what AFSL holders must have in place to manage cyber risk (i.e., what is adequate in all cases), the decision does establish that a standard of care is required.

The Court rejected the suggestion that the relevant standard for assessment of adequate cyber risk management should be determined by "public expectation". The public is entitled to expect that appropriate cyber security measures are taken, the controls, measure and risk management relating to cybersecurity risk should not be assessed in this way.

Instead, the Court took the view that cyber risk management is a highly technical area of expertise and concluded that **"the assessment of the adequacy of any particular set of cyber risk management systems requires the technical expertise of a relevantly skilled person".**

As a guide to what is not adequate, this case provides the following examples:

- computer systems which did not have up-to-date antivirus software installed and operating;
- no filtering or quarantining of emails;
- no backup systems in place, or backups not being performed; and
- poor password practices including lack of multi-factor authentication, sharing of passwords between employees, use of default passwords, passwords and other security details being held in easily accessible places or being known by third parties.

Wide-ranging implications for organisations more broadly

It is important that all organisations consider the approach to cyber risk management and adequacy in light of this case. While this case was focussed on the obligations of AFSL holders, we expect that ASIC will also use its oversight powers to identify whether directors of any company that fails to adequately consider cyber risk, are in breach of their obligations.

Similarly, this decision is likely to inform the enforcement approach that other regulators take to cyber security issues. Those organisations that are required to comply with APRA's Prudential Standard CPS 234 – Information Security or which are affected by the new critical infrastructure requirements, should take note of this emerging standard for developing management of cyber risk.

On 5 May 2022, the date the ASIC v RI Advice judgment was delivered, ASIC's deputy chair, Sarah Court, made the following statement in relation to *ASIC v RI Advice*: *"ASIC strongly encourages all entities to follow the advice of the Australian Cyber Security Centre and adopt an enhanced cybersecurity position to improve cyber resilience in light of the heightened cyber-threat environment"*. This statement goes well beyond only AFSL holders and indicates ASIC's intention to promote this standard of cybersecurity across the board.

As the subject of multiple cyber incidents over an extended period, ASIC was successful in pursuing this test case on the question of cybersecurity expectations. From here, ASIC now has a benchmark with which it can pursue other entities, as observed by equivalent regulators in overseas jurisdictions.

By considering cybersecurity risk management a necessary investment, rather than an afterthought, organisations can avoid significant costs in the aftermath of an event. What started out as a series of IT issues ultimately escalated to becoming a high-profile ASIC prosecution involving legal compliance and reputational risk management issues.

In this case, RI Advice not only incurred costs in relation to the regulator investigation, responding to litigation and the remediation costs for uplifting their cyber security. In the absence of admissions made, if ASIC had to prove its case, the Court may have made additional orders including imposing significant penalties.

That being said, as risks relating to cybersecurity and the responsive measures to it are constantly evolving, organisations have an ongoing obligation to cast their minds to cybersecurity beyond initial setup. To ensure that this obligation is met, organisations should be conducting regular reviews of their infrastructure, ensuring that it is up to date and appropriate in the current circumstances.

This decision serves as a useful legal precedent for establishing a nexus between cybersecurity risk management and compliance with broader professional obligations. It may also form the basis of further precedent that applies across the professional services industry more broadly in terms of their own data handling and cyber security practices.

Event Report: CAMLA Young Lawyers Networking Panel Event 2022

The CAMLA Young Lawyers Committee held their annual networking event on 24 May 2022, hosted at McCullough Robertson.

The hybrid event allowed attendees both online and in person to hear from our wonderful panellists about their experiences networking and all the paths that led to where they are today. After the formal part of the evening, attendees enjoyed drinks and canapes, putting their new networking skills to the test.

The audience heard some insightful stories and tips about networking, how to be authentic when making connections and how these skills and experiences helped our panellists throughout their careers.

Some sage advice the attendees took from the event include the reminder to back yourself when networking, being persistent when trying to make connections and an offer for coffee goes a long way when you want to learn about someone's career path.

The CAMLA Young Lawyers Committee would like to again thank panellists **Rebecca Lindhout** (Special Counsel at McCullough Robertson), **Dan Roe** (Senior Attorney, Original Production at The Walt Disney Company), and **Antonia Rosen** (Legal Counsel at News Corp Australia) for participating in the event.

CAMLA Board Member Rebecca Lindhout also congratulated the winners for the CAMLA Essay Competition:

Adam Lukacs (University of Queensland), for his piece (published in this edition) on source confidentiality under siege;

Nadine Mattini (University of Sydney) , for her piece (published in this edition) on the serious harm threshold in physician review defamation disputes; and

Julian Sanders (University of Western Australia), for his piece on music copyright and the doctrine of objective similarity.

The evening was moderated by **Calli Tsipidis** (Chair of the CAMLA Young Lawyers Committee, Foxtel) with help on the night from **Jessica Norgard** (nbn), **Anna Kretowicz** (Judge's Associate), **Nicola McLaughlin** (nbn) and **Erin Mifsud** (eSafety Commissioner).

Thank you again to our amazing panellists and McCullough Robertson for generously hosting the evening. It was a great night with engaging conversation and a few laughs. We look forward to seeing you at our next CAMLA Young Lawyers event.

All Eyes on the Anti-Trolling Bill, But What About the Online Safety Act?

David Kim, Banki Haddock Fiora, comments on why the eSafety Commissioner's expanded remit is on a collision course with the world of defamation.

Introduction

The last few months have seen a flurry of activity around the *Social Media (Anti-Trolling) Bill 2022* (Cth) (**Bill**), which was accepted in all quarters as being in fact an attempt, at the federal level, to make sweeping changes to defamation law, specifically as it applies to material posted to social media platforms. The Bill lapsed upon Parliament being prorogued on 11 April 2022, but not before it was thoroughly excoriated by an ensemble of defamation practitioners and experts, a judge, and various other stakeholders. With the recent change in government, it is likely that the Bill will not be passed without substantial amendments, if it is passed at all.[1]

The Online Safety Act

The excitement and consternation around the Bill have overshadowed another piece of federal legislation with ramifications for the world of defamation, namely the *Online Safety Act 2021* (Cth) (**OSA**). The OSA overhauls and replaces, in its entirety, the *Enhancing Online Safety for Children Act 2015* (Cth) (**EOSCA**), and significantly expands the powers and responsibilities of the eSafety Commissioner. Previously, under the EOSCA, the eSafety Commissioner's role was focused on the investigation and regulation of "cyber-bullying material targeted at an Australian child". That remit has now been expanded to include the investigation and regulation of "cyber-abuse material targeted at an Australian adult".

The OSA provides that if the eSafety Commissioner is satisfied that material is "cyber-bullying material targeted at an Australian child" or "cyber-abuse material targeted at an Australian adult" it may issue a removal notice to a social media service provider, a designated internet service provider, the provider of a relevant electronic service, a hosting services provider or (in the case of cyber-abuse material) an end-user.[2] Removal notices issued by the eSafety Commissioner must be complied with within 24 hours, with non-compliant persons being liable to civil penalties, formal warnings and being named by the eSafety Commissioner in public statements.[3] A complainant may apply to have the Administrative Appeals Tribunal review a decision to refuse to issue a removal notice,[4] and, conversely, a relevant provider or an end-user who posted the alleged problematic material may apply to have the Administrative Appeals Tribunal review a decision to issue a removal notice.[5]

An overlap with defamation law?

On their face, the concepts of "cyber-abuse material targeted at an Australian adult" and "cyber-bullying material targeted at an Australian child" seem expansive enough to encompass at least some kinds of online defamation. Already, it has been suggested that the OSA can and should be used to rapidly remove online defamatory material.[6] The current eSafety Commissioner, Julie Inman Grant, however, has advocated for the contrary view that the eSafety Commissioner's powers should not be understood as extending to matters that fall within the sphere of defamation law.[7] In evidence given to the Senate Standing Committee for Legal and Constitutional Affairs (**LACA**), the eSafety Commissioner explained that Parliament had dealt with the overlap issue by building into the definitions of cyber-abuse material a threshold that screens out defamatory material.[8]

---

1 Senate Standing Committee for Legal and Constitutional Affairs, Parliament of Australia, *Social Media (Anti-Trolling) Bill 2000 [Provisions]* (Report, March 2022) 65-6 [1.65]-[1.66].

2 *Online Safety Act 2021* (Cth) ss 65-6 and 88-90.

3 *Online Safety Act 2021* (Cth) ss 67-8, 71-3 and 91-3.

4 *Online Safety Act 2021* (Cth) s 220(4)-(5).

5 *Online Safety Act 2021* (Cth) s 220(2)-(3).

6 Meta, Submission No 7 to the Senate Standing Committee for Legal and Constitutional Affairs, *Social Media (Anti-Trolling) Bill 2000 [Provisions]* 10.

7 Evidence to the Senate Standing Committee for Legal and Constitutional Affairs, Parliament of Australia, Canberra, 10 March 2022, 12-5 (Ms Julie Inman Grant, eSafety Commissioner).

8 Ibid 19. It is unclear what the Office of the eSafety Commissioner's current position is. In LACA's examination of the eSafety Commissioner on 10 March 2022, the eSafety Commissioner indicated that 33 percent of the cyber-abuse material complaints received by her office "concern potentially defamatory material and therefore do not meet the threshold for serious adult cyberabuse under our scheme". On the other hand, Mr Toby Dagg, an Executive Manager at the Office of the eSafety Commissioner, acknowledged that "there may be some matters that reach the threshold of adult cyberabuse that could also be considered potentially defamatory, but we are dealing with that as adult cyberabuse, not as defamation, through the act". Also, the website of the Office of the eSafety Commissioner has a page that discusses the differences between serious online abuse and defamation and notes that the threshold for cyber abuse material is high, but acknowledges that "in some cases material posted which might be defamatory could ALSO meet the threshold of adult cyber abuse... this means an Australian could come to eSafety to have content removed, and or also elect to take defamatory action": https://www.esafety.gov.au/newsroom/blogs/difference-between-serious-online-abuse-and-defamation.

A matter of definitions

Section 6 of the OSA essentially provides that material will be "cyber-bullying material targeted at an Australian child" if an ordinary reasonable person:

a) would conclude that the material was intended to have an effect on a particular Australian child; and

b) would be likely to have the effect on the Australian child of seriously threatening, seriously intimidating, seriously harassing or seriously humiliating the Australian child.[9]

Section 6 screens out some but not all kinds of defamatory material. Section 6 screens out defamatory material that is not intended to have an effect on a particular Australian child, and defamatory material which is unlikely to have certain effects on an Australian child. It is, however, possible to conceive of defamatory material that would come within the ambit of section 6.

The definition of "cyber-abuse material targeted at an Australian adult" is set out in section 7 of the OSA and is comprised of four separate integers (each a necessary integer). The two integers that are most relevant for present purposes are as follows:

> An ordinary reasonable person would conclude that it is likely that the material was intended to have an effect of causing serious harm to a particular Australian adult (s 7(1)(b)); and
>
> An ordinary reasonable person in the position of the Australian adult would regard the material as being, in all the circumstances, menacing, harassing or offensive (s 7(1)(c)).

The first of the above integers focusses on the likely intention of the material. It also builds on the concept of "serious harm", a term that is defined in section 5 of the OSA as "serious physical harm or serious harm to a person's mental health, whether temporary or permanent". The term "serious harm to a person's mental health" is, in turn, defined as "including (a) serious psychological harm; and (b) serious distress; **but does not include mere ordinary emotional reactions such as those of only distress, grief, fear or anger**".

It is unclear whether the reference to a threshold by the eSafety Commissioner in her evidence to LACA is a reference to the bolded words above, or to the combined effect of the two ordinary reasonable person integers. However, in either case, and with respect to eSafety Commissioner, it does not appear to be the case that the definition of either cyber abuse material contains a threshold that effectively excludes all defamatory material. It is possible for defamatory material to be intended to have an effect of causing serious distress (and, for that matter, serious psychological harm), and, at the same time, menacing, harassing or offensive.[10]

In the case of an Australian adult, what is screened out by the definition of cyber-abuse material is defamatory material that was not intended or likely intended to cause serious physical harm or harm to a person's mental health. It follows that defamatory material that only causes reputational damage or only causes reputational damage and economic loss would appear to be screened out.

Cyber abuse material also does not include defamatory material that is intended or likely intended to cause mere ordinary emotional reactions and nothing more.

Finally, the definition of cyber-abuse material also screens out defamatory material that is not menacing, harassing or offensive.

The definitions in the OSA do not, in their terms, exclude defamatory material from the regulatory framework administered by the eSafety Commissioner. The better view is that there is a partial overlap between material regulated by the OSA and material actionable under defamation law.[11]

Takedown fast track

This overlap is potentially significant.

At present, apart from the OSA, there is no quick or simple method for achieving the removal of online defamatory material. Interlocutory injunctions to restrain defamations are rarely granted, and there is anecdotal evidence to suggest that social media services providers are reluctant to take down material posted on their platforms in the absence of a vindicatory court judgment.

A complaint to the eSafety Commissioner may however achieve a takedown result in a matter of days, and may obviate the need to commence defamation proceedings entirely. The eSafety Commissioner may also use their powers to issue removal notices to various persons along the "publication chain", avoiding the problems associated with enforcing injunctions against entities based outside Australia.

Moreover, approaching the eSafety Commissioner is a particularly attractive option if a person targeted by defamatory material is more concerned with securing the prompt take down of that material than with achieving vindication, receiving an apology or obtaining monetary compensation.

---

9 *Online Safety Act 2021* (Cth) s 6.

10 Whether material is "offensive" is to be determined by having regard to matters set out in s 8 of the *Online Safety Act 2021* (Cth).

11 The explanatory memorandum to the *Online Services Bill 2021* (Cth) notes (on page 70) that the definition of "cyber-abuse material targeted at an Australian adult" "is not intended to capture 'repuational harm' caused by defamatory material" but acknowledges that "defamatory material may be determined to be 'cyber-abuse material targeted at an Australian adult' where an intent to cause serious mental or physical harm to a person can be established".

12 *Sattin v Nationwide News Pty Ltd* (1996) 39 NSWLR 32; *Sullivan v Moody* (2001) 207 CLR 562; *Tame v New South Wales* (2002) 211 CLR 317.

That said, the usefulness of the removal notice regime set out in the OSA is likely to be limited to so-called "backyarder disputes", particularly those that involve a level of harassment or an ongoing campaign intended to cause serious distress or psychological or physical harm. The removal notice is unlikely to be an appropriate vehicle to seek, for example, takedowns in respect of online news articles. This is because it will generally be difficult to satisfy the eSafety Commissioner that the ordinary reasonable person would conclude that such material had the requisite intention or (in the case of an Australian adult) the requisite likely intention.

Possible teething problems

The overlap also poses more questions than answers. Two questions in particular come to mind.

First, there is a line of authority that states (or arguably states) that the appropriate cause of action for reputational damage is defamation, and that the defences developed over time in defamation cannot be sidestepped by using another cause of action as a vehicle to obtain remedies in respect of reputational damage.[12] Is that line of authority a basis for actionable defamatory material being excluded from the operation of the OSA? The tentative view of the author is that it does not, as there are points of distinction here that make any application of that line of authority doubtful. For example, standing to lodge a complaint with the eSafety Commissioner is not equivalent to a cause of action, and the eSafety Commissioner exercising its discretion to issue a person with a removal notice is not really a remedy either. Moreover, the OSA does not create liability for publication on the part of a person publishing cyber-abuse or cyber-bullying material. Finally, and perhaps most importantly, the regulatory framework administered by the eSafety Commissioner is a statutory one and the legislature is not inhibited from enacting a regulatory framework that overlaps with defamation law.[13]

The second question is whether the eSafety Commissioner can or should, in issuing removal notices, have regard to the principles governing the granting of interlocutory injunctions in defamation cases. Various cases suggest that those principles cannot be circumvented by a litigant bringing what is in effect a defamation action in the guise of some other cause of action.[14] However, again, there are points of distinction here that make the application of those principles uncertain. If those principles are applied to the removal notice regime set out in the OSA, they will generally require the eSafety Commissioner to be satisfied of the falsity of imputations conveyed by cyber-bullying or cyber-abuse material, and the eSafety Commissioner has already indicated that her office does not have the resources to undertake such a fact-finding exercise.[15]

Conclusion

Whether by default or by design, the OSA has potentially significant implications for defamation practice. The OSA does not reform defamation law but it does create an expedited route to achieving take down outcomes in respect of at least some kinds of defamatory material. The OSA also raises the spectre of defamatory material being taken down without regard to whether the publisher is able to justify the imputations conveyed by that material, or rely successfully on any of the other defences enshrined in defamation law. It remains to be seen to what extent, if any, established defamation law principles can and will guide the eSafety Commissioner's exercise of her extensive powers under the OSA.

---

13 *Global Sportsman Pty Ltd v Mirror Newspapers Pty Ltd* (1984) 2 FCR 82; *TCN Channel Nine Pty Ltd v Ilvariy Pty Ltd* (2002) 71 NSWLR 323.

14 *Service Corp International plc v Channel Four Television Corp* [1999] EMLR 83; *Swimsure (Laboratories) Pty Ltd v McDonald* [1979] 2 NSWLR 796; *Church of Scientology of California Inc v Reader's Digest Services Pty Ltd* [1980] 1 NSWLR 344.

15 Evidence to the Senate Standing Committee for Legal and Constitutional Affairs, Parliament of Australia, Canberra, 10 March 2022, 19 (Ms Julie Inman Grant, eSafety Commissioner).

Therapeutic Goods Advertising Code Gets a Makeover

Jaimie Wolbers, Simone Mitchell and **Jonathan Kelp** (MinterEllison) discuss what the new Therapeutic Goods Advertising Code 2021 will mean for advertisers.

On 1 January 2022, the new *Therapeutic Goods Advertising Code 2021 (Cth)* (**Code**) came into effect. The Code sets out the requirements for the promotion of therapeutic goods (such as medicines and medical devices) in Australia with a view to ensuring that such advertising, promotes the quality use of products, is socially responsible and does not mislead or deceive consumers.

In Australia, the majority of medical devices, as well as most medicines available for over-the-counter sale, can be advertised to consumers. However, the promotion to the public of prescription medicines, and certain pharmacist only medicines, is prohibited. While Australia dealt with the Omicron COVID-19 wave over the summer months of 2021/22, significant changes were introduced to Australia's therapeutic goods advertising regime through the implementation of the new Code.

Despite coming into effect on 1 January 2022, the life sciences sector has been provided with a six month transition period during which they may choose to comply with either the 2018 or 2021 versions of the Code. However, from 1 July 2022, all therapeutic goods advertising directed to consumers will need to comply with the new Code. Advertisers who do not comply risk committing an offence under section 42DM of the *Therapeutic Goods Act 1989 (Cth)* (**Act**) or breaching the civil penalty provision in section 42DMA, each of which may attract significant penalties.

Key features of the new Code include changes to the mandatory statements that must be included in advertisements, an expanded list of products that may be provided as samples to the general public, and clarification that the use of influencers (ie individuals who are paid or otherwise incentivised) to promote therapeutic goods is not permitted. We set out a summary of these key features below.

Updated mandatory statements

One of the notable additions to the new Code is a requirement to prominently display or communicate the following statement in advertisements for products that cannot be directly purchased by a consumer, and that are supplied through healthcare professionals:

> "*This product is not available for purchase by the general public*"

We expect that the introduction of this mandatory statement is tied to one of the key objects of the Code (set out at section 2), which is to ensure that advertisements for therapeutic goods support informed healthcare choices. It also aligns with the existing requirements in the Code to ensure that any advertisement for a therapeutic good does not:

Key Takeouts

- The changes to the Code will affect how therapeutic goods can be promoted to consumers in Australia. Changes include amendments to mandatory statements which must be included in advertising.
- The deadline for ensuring compliance with the new Code is 30 June 2022.
- Sponsors and advertisers should not delay in reviewing existing and future marketing campaigns for compliance with the new Code.

- delay or discourage persons from seeking necessary medical attention; or
- delay or discourage persons from undertaking treatment prescribed by a medical practitioner.

Advertisements for products that are not available for direct purchase by consumers are not required to comply with the more prescriptive requirements set out in Part 4, Division 3 of the Code. This is a similar situation for:

- advertisements for pharmacist only medicines (therapeutic goods consisting of or containing a substance included in Schedule 3 and Appendix H of the Poisons Standard) which must prominently display or communicate the statement:

  "*Ask your pharmacist about this product*"; and

- short form advertisements (radio spots of ≤ 15 seconds or text only advertisements of ≤ 300 characters, where there is no reasonable capacity to include a picture, logo or other imagery as part of the advertisement) which must prominently display or communicate the statement:

  "Always follow the directions for use"

Part 4, Division 3 sets out mandatory statements and required information that must be included in all other advertisements for medicines, medical devices and other therapeutic goods. There are additional requirements, including to prominently display and communicate any health warnings, in circumstances where the advertisement facilitates the direct purchase or supply of the therapeutic goods without the consumer having an opportunity to inspect the product (i.e. advertisements published on websites, social media pages or via a software application through which a transaction for the product may be conducted).

Samples

The Code now includes an expanded list of therapeutic goods that offer samples by way of an advertisement. An advertisement about therapeutic goods may now include or offer the following therapeutic goods as samples (provided they are included on the Australian Register of Therapeutic Goods and do not include a substance included in Schedules 2, 3, 4 or 8 of the Poisons Standard):

- personal lubricants;
- COVID-19 rapid antigen tests for self-testing;
- disinfectants;
- face masks and gloves for preventing the transmission of disease in persons;
- hand sanitisers;
- lancets and blood glucose strips for use in connection with measuring blood glucose;
- nicotine replacement therapies administered by oromucosal or transdermal means, including sprays, patches, gums, lozenges, sachets and tablets;
- oral hygiene products, including toothpaste, mouthwash and interdental brushes;
- oral rehydration products;
- tampons and menstrual cups; and
- wound care dressings for superficial wounds, including first aid items and antiseptics.

This adds to the existing list which was previously limited to:

- condoms;
- goods that are / contain a sunscreen;
- stoma devices for self-management; and
- continence catheter devices for self-management.

Testimonials & Endorsements – implications for influencers

Importantly, the new Code also consolidates the requirements regarding testimonials and endorsements into section 24. Although the requirements relating to testimonials and endorsements largely remain unchanged, the new Code clarifies that social media influencers who have received (or will receive) payment or valuable consideration in order to provide a testimonial are considered to be persons engaged in the marketing of therapeutic goods. The Code prohibits the use of testimonials from persons engaged in the marketing of therapeutic goods and, therefore, it is now clear that sponsors and advertisers of therapeutic goods must not engage or use influencers to provide testimonials promoting therapeutic goods. This should hopefully lead to a change in the way in which therapeutic goods are advertised on social media.

Event Report: CAMLA Young Lawyers Music Law 301 Seminar

Jess Millner (MinterEllison, CAMLA Young Lawyers Committee representative)

On 11 April 2022 Marque Lawyers hosted the CAMLA Young Lawyers Music Law 301 Seminar. The 301 seminar was a fabulous way to round out the CAMLA Young Lawyers Music Seminar Series. **Michael Bradley** and **Emma Johnsen** of Marque Lawyers were joined by artist and producer **Jack River** (aka Holly Rankin) to discuss some of the current issues facing the music industry. It was an insightful discussion covering the impact of the pandemic on music touring and events, the ins and outs of record label deals, the rise of NFTs in the music industry and the "Beneath the Glass Ceiling" campaign.

The seminar was a unique opportunity for young lawyers to gain valuable industry insights.

Thank you very much to the panel for an engaging and open discussion. For those that missed it the seminar was recorded and it is available to CAMLA members on the CAMLA website – check it out!

Event Report: Defamation on Digital Platforms

In eager anticipation of the recommendations of the Defamation Working Party in relation to 'Stage 2' of the Defamation Law Reforms, CAMLA gathered together a panel of some of Australia's pre-eminent defamation experts for a lively discussion on defamation on digital platforms.

The panel, skilfully moderated by Marlia Saunders (Thomson Geer) and Jake Blundell (Bank Haddock Fiora), included David Rolph (University of Sydney), Sue Chrysanthou (153 Phillip Barristers), Matthew Lewis (Level 22 Chambers), and Andrew Stewart (Baker McKenzie).

Audience members both in person at Thomson Geer in Sydney and watching via live-stream were treated to a lively debate and various perspectives on the subject, although there were some areas of consensus. The panellists discussed that the *Social Media (Anti-Trolling) Bill,* described as a confusing effort by the Commonwealth to intervene on a single facet of defamation law, is likely behind us following the recent election result. The panel also discussed issues left unresolved post-Voller, noting that the interaction of defamation on digital platforms with other areas of law and existing complaints mechanisms will require an integrated and holistic approach to addressing online harms.

Turning to what other approaches might be worth exploring, the panel discussed various approaches adopted overseas, noting that the solutions under consideration in Australia in 2022 were introduced nearly 10 years ago in the United Kingdom. They also explored some innovative possible solutions, such as a new form of an innocent dissemination defence available to digital platforms, and a process similar to site blocking orders available against ISPs, whereby a complainant could apply for a court order for content removal, to be heard by a judge in a specialist list.

CAMLA thanks the panellists for an engaging and thought-provoking evening, and our hosts Thomson Geer for supporting a wonderful event.

Event Report: CAMLA Cup

Jessica Norgard (Senior Legal Counsel, nbn, CAMLA Young Lawyers Committee representative)

250 keen media and communications lawyers and aficionados gathered at Sky Phoenix for a reunion three years in the making: the CAMLA Cup was back in style. Ready with a barrage of energy were Quizmaster & MC extraordinaires Ryan Grant and Debra Richards, who guided the evening with their quick wit and topical questions. A few rounds, plus some "Who Am I's" later, the "Quaranteam" from Addisons emerged triumphant. But don't worry, in true CAMLA style – every team went away with a prize (even if, for one unlucky bunch, it was an actual wooden spoon!)

It was an evening of wonderful catch-ups and camaraderie, and epic trivia team names.

As usual, a huge thanks to Cath Hill, the judges, quiz-drafters and all the firms and companies who donated prizes, and to all those who attended, including:

Addisons | Ashurst | Baker McKenzie | Banki Haddock Fiora Bird & Bird | Clayton Utz | Corrs Chambers Westgarth Creative Lawyers | Dentons | Foxtel | Gilbert + Tobin Holding Redlich | Johnson Winter & Slattery Level 22 Chambers | McCullough Robertson | MinterEllison Netflix | SBS | Thomson Geer | Webb Henderson

To Be or Not to Be. Who Can Be an Inventor?

Helen Macpherson (Baker McKenzie Sydney), **Tanvi Shah** (Baker McKenzie, London) and **Avi Toltzis** (Baker McKenzie, Chicago) discuss the Thaler litigation, and the questions it raises about the recognition of AI as an inventor under patent law.

As we all know, digital technologies have infiltrated and transformed all facets of industry and commerce, leading to the creation and use of tech-based IP across both traditional and non-traditional tech sectors.

Digital technologies come in many different forms including blockchain, cloud computing, artificial intelligence (**AI**), data analytics and the Internet of Things (**IoT**) (or what used to be called wireless sensor networks). The digital technologies available to us today and in the future are at the forefront of innovation. As a result, they are pushing the boundaries of IP laws, giving rise to novel issues impacting IP strategies including what types of IP are best placed to protect and monetise digital technologies, how you frame these rights (for example what you patent and how you draft your patents) and how to enforce your IP rights. A key issue for digital technologies that facilitate new modes of creation is that of who or what can be legally recognised as the creator or inventor of such technologies. This is a fundamental issue for many digital technologies, and none more so than AI, in which there is minimal human input.

Last year, the Federal Court of Australia became the first court worldwide to recognise AI as being capable of being an "inventor" of a patent. That decision of a single judge of the Federal Court of Australia has now been overturned by a unanimous decision of the Full Federal Court (see Commissioner of Patents v Thaler [2022] FCAFC 62). In this article, we explain the technology the subject of the decision and provide an overview of the Full Court's rationale for overturning the single judge's decision. We then provide a global perspective, considering the counterpart decisions in the United Kingdom, the United States and the European Union.

The technology: DABUS

Dr Stephen Thaler, a Missouri-based engineer, filed patent applications in various patent offices around the world for inventions relating to food and beverage containers and methods for attracting enhanced attention. In each of the patent applications, Dr Thaler identified an AI system he created called DABUS (an acronym for "device for the autonomous bootstrapping of unified sentience") as the sole inventor.

Dr Thaler argued that DABUS, which he characterised as a "creativity machine", was programmed as a series of neural networks and was not created to solve any particular problem nor trained on any data especially relevant to the inventions. Rather, DABUS independently conceived of the invention, and on this basis, Dr Thaler argued that DABUS, not any human, was the true inventor.

The Australian Position

So what was the Australian Full Court's rationale for overturning the single judge's decision? Ultimately, it all came down to statutory interpretation, which is primarily a text-based exercise but which can be informed to a certain extent by policy considerations. In the Full Court's view, the use of the word "person" in the key statutory provision (section 15 of the Australian Patents Act 1990 (**Patents Act**) which addresses the issue of who may be granted a patent) meant a "natural person". The Full Court considered that no other provision in the Patents Act was inconsistent with this interpretation of section 15, and that this interpretation was consistent with centuries of patent law which had proceeded on the assumption that only a natural person could be an inventor. In discussing the latter point, the Full Court referenced the High Court of Australia's decision in *D'Arcy v Myriad Genetics Inc* (2015) CLR 334 where the majority stated that an invention is something which must be brought about by human action.

The Full Court recognised that the debate as to the role of AI in the patent context was "important and worthwhile", but stated that these considerations were not relevant in the present case which required consideration of the interpretation of the relevant statutory provisions. In this regard, the Full Court cautioned against approaching the task of statutory interpretation by reference to what might be regarded as desirable policy, imputing that policy to the legislation, and then characterising that as the purpose of the legislation. The Full Court also did not consider that, if AI was not accepted to be an inventor, no invention devised by AI would be capable of being the subject of a granted patent. While in the present case it was an agreed fact that the AI system was the inventor of the invention the subject of the patent application, the characterisation of a person as an inventor is a question of law. The question of whether the application that was the subject of this appeal had a human inventor had not been explored and so remained undecided.

The Global Perspective

The Full Court's decision brings Australia into line with that of other major jurisdictions such as the UK, US and EU where Dr Thaler also applied for patents with DABUS designated as the inventor.

The United Kingdom

In September 2021, the UK Court of Appeal dismissed the appeal seeking to overturn the first instance court's decision that the UK Intellectual Property Office (**IPO**) was correct to regard Dr Thaler's applications as withdrawn for his failure to identify a natural person as the inventor of the patent in accordance with sections 7 and 13 of the UK Patents Act 1977. LJ Arnold (joined by Lady Justice Laing, writing separately) ruled that the UK IPO was entitled to deem the application withdrawn as a result of Dr Thaler's designation of DABUS as the inventor. LJ Birss concurred that an AI system could not be the inventor of a patent but concluded that the UK IPO was not empowered to deem an application withdrawn on the basis that the applicant had named an AI system as the inventor.

So, while all three judges on the panel agreed that the inventor of a patent must be a natural person, LJ Birss dissented from his peers on the legal effect of an applicant

identifying an AI system as the inventor on a patent application under section 13(2). Under this subsection, the applicant must name the person they "believe[] to be the inventor" and indicate "the derivation of [the applicant's] right to be granted the patent" if the applicant is someone other than the inventor. LJ Birss found that Dr Thaler, in naming DABUS as the inventor and explaining how he programmed, owned, and operated DABUS, had complied with section 13(2) because he sincerely believed DABUS to be the inventor of the patent. Accordingly, Dr Thaler's designation of DABUS as the inventor did not constitute grounds for the UK IPO to refuse the patent, even though LJ Birss accepted that section 7 required the inventor of a patent to be a natural person.

LJ Arnold, while agreeing with LJ Birss that it was outside the remit of the UK IPO to investigate the factual correctness of statements of inventorship, rejected the notion that section 13(2) merely required an earnest declaration of who the applicant believed was the inventor. Because Dr Thaler's statement that DABUS invented the patent was, on its face, legally impossible, it could not comply with section 13(2). Accordingly, LJ Arnold (and by agreement LJ Laing) concluded that Dr Thaler, by his failure to identify a legally plausible inventor of the patent, caused the application to be withdrawn.

Notably, the conclusion that an inventor must be a natural person was arrived at "without any need to examine the policy arguments raised by both parties." and, as stressed by LJ Birss, the case simply turned on "the correct way to process patent applications through the Patent Office" and not on any larger questions around the patentability of AI-created inventions.

The United States

A few weeks before the UK Court of Appeal's decision, the District Court for the Eastern District of Virginia became the first US court to consider whether AI can be named as the inventor of a patent.

Judge Leonie Brinkema disposed of the appeal summarily by finding that the US Patent and Trademark Office (**USPTO**) should be afforded Skidmore deference, which accords an agency latitude to determine how to administer its statutory duties, as long as its position is reasonable in light of the relevant statute.

While Judge Brinkema concluded that the application of Skidmore deference was dispositive of Dr Thaler's claim, she nonetheless proceeded to analyse, and ultimately endorse the USPTO's legal conclusions. At the outset Judge Brinkema observed that the *America Invents Act of 2011* amended the definition of "inventor" in the section 100(f) of the Patent Act to mean "the individual...who invented or discovered the subject matter of the invention." Judge Brinkema then cited a recent Supreme Court decision that interpreted the term "individual" (as used in the *Torture Victim Protection Act*) to refer exclusively to a natural person.

She also examined how the term "individual" was used in the context of the Patent Act and found that it could only be consistent with the construction limited to human beings. For example, under section 115(b)(2), the inventor was to include a statement that he or she believes himself or herself to be the original inventor, a phrase rendered meaningless if applied to a being incapable of belief like an AI. As the conventions of statutory construction presumed a term to have a consistent meaning throughout a statute, the term "individual" was held to have the same meaning in other Patent Act provisions.

Judge Brinkema then turned to a pair of recent Federal Circuit decisions interpreting the Patent Act and holding that inventors must be natural persons. Although these decisions examined the contention that a sovereign state or a corporation, respectively, could constitute an inventor, they corroborated Judge Brinkema's other findings and were considered highly persuasive.

Having concluded that the text of the Patent Act, along with cases interpreting it and similar language, supported a limited definition of inventor, Judge Brinkema concluded her judgment giving short shrift to Dr Thaler's policy arguments. Without assessing the merits of the policy arguments themselves — that conferring inventorship on AI systems would "incentivize the development of AI capable of producing patentable output" — she conceded that such contentions could not prevail in the face of the statute's plain language.

European Patent Office

The Receiving Section of the European Patent Office (**EPO**) has also recently refused Dr Thaler's patent application. It did so for two reasons. First, it concluded that only a human inventor could be an inventor within the meaning of the European Patent Convention (**EPC**). For this reason, designating a machine as inventor did not comply with the requirements set out in Article 81 and Rule 19(1) of the EPC. Secondly, the Receiving Section was of the opinion that a machine could not transfer any rights to the applicant. The Receiving Section considered therefore that the statement that the applicant was successor in title because they owned the machine did not satisfy the requirements of Article 81 EPC in conjunction with Article 60(1) EPC.

The appeal of the refusal by the Receiving Division of the EPO was heard by the EPO's Technical Board of Appeal in December 2021. The Technical Board dismissed the appeal, but their written reasons are yet to be published.

Conclusion: AI as an inventor

So you can see that in these recent decisions, courts and patent offices worldwide have grappled with the question of whether a patent application can name an AI system as its inventor. The decisions to date share a common feature: careful examination of the text of the governing statutes and conventions, resulting in conclusions that rendered assessment of the underlying policy considerations unnecessary. However, this is not yet the end of the road for Dr Thaler who has made a special leave application to the High Court of Australia and applied for permission to appeal to the UK Supreme Court, as well as appealing to the US Federal Circuit.

Relevantly, important questions remain unanswered when it comes to patents-based on AI technology. The Australian Full Court concluded their judgment by briefly listing some of the many questions that arise for consideration in the context of AI and inventions. These questions included:

- As a matter of policy, should a person who is an inventor be redefined to include AI?

- If so, to whom should a patent be granted in respect of its output? For example, the owner of the machine upon which the AI software runs, the developer of the AI software, the owner of the copyright in its source code or the person who inputs the data used by the AI to develop its output? The answer to this question will be critical in determining who reaps the windfalls of the AI revolution.
- If AI is capable of being recognised as an inventor, should the standard of inventive step be amended such that it is no longer judged by reference to the knowledge and thought processes of the hypothetical uninventive skilled worker in the field? Questions of validity such as inventiveness (as well as sufficiency/enablement) are often resolved with reference to a hypothetical skilled team. If we accept that the notional skilled team has access to — or perhaps even is — an AI device, their ability to solve technical problems would likely be considerably enhanced, both quantitatively and qualitatively. And while we might observe that calculators, computers, high-throughput sequencing and other innovations enable skilled teams to expand their capabilities, we must also accept none of these technologies are even arguably capable of independent inventiveness — unlike AI, the potential of which is yet to be fully understood.
- What continuing role might the ground of revocation for false suggestion or misrepresentation have, in circumstances where the inventor is a machine?

The Australian Full Court recognised the urgency of resolving these questions. It is, however, yet to be seen how or when — as these issues were put to the courts in the recent DABUS cases — and until then "to be or not to be, that is the question".

Event Report: CAMLA Young Lawyers Music Law 201 Seminar

Nicola McLaughlin (Legal Counsel, nbn, CAMLA Young Lawyer Committee Secretary)

Springboarding off the first event in the Music and the Law Series, the CAMLA Young Lawyers Committee were thrilled to kick off CAMLA's first hybrid event for 2022 with its very own Music Law 201. The event boasted a lively and practical discussion about the complexities of collective licensing and the role of copyright collecting societies in the music industry.

Key topics of discussion included:

- the different roles of each collecting society;
- the intentions behind creating OneMusic Australia (the joint initiative between APRA AMCOS and PPCA);
- whether you need a licence to perform or record a cover song;
- whether the everyday TikTok user requires a licence to incorporate music in their posts; and
- how music royalties flow from streaming services.

Our esteemed panellists included Lynne Small, (Chief Operating Officer, Australian Recording Industry Association and Phonographic Performance Company of Australia) Kate Haddock (Partner, Banki Haddock Fiora) and Chris Johnson (Director of Legal Services, APRA AMCOS). Following CAMLA's first in-person event since the second wave of COVID-19, the audience and panellists enjoyed catching up over some drinks and nibbles provided by our gracious host, Banki Haddock Fiora.

The CAMLA Young Lawyers Committee would like to take this opportunity to thank Banki Haddock Fiora and our expert panellists for donating their time and answering an abundance of questions from the lively audience.

Special thanks also to our event moderators, Isabella Boag Taylor (Associate, Bird & Bird) and Belyndy Rowe (Senior Associate, Sainty Law)

Out of Sight But Not Out of Jurisdiction – Application of the *Privacy Act 1988* (Cth) to Extra-Territorial Companies

Marlia Saunders, partner and **Jessie Nygh**, lawyer at Thomson Geer, discuss the recent findings of the Full Federal Court in *Facebook Inc v the Australian Information Commissioner* and what it means to 'carry on business' in Australia in the digital age.[1]

Introduction

It may, for the average Australian, feel like the Cambridge Analytica scandal is but a distant memory. Mark Zuckerberg apologised, Facebook rebranded to Meta and the Netflix smash hit *The Social Dilemma* highlighted how social media companies use data to target advertising to users. Nevertheless, our courts are still determining the parameters for the use of personal data by corporations like Facebook. In a recent decision, the Full Court of the Federal Court of Australia clarified that Facebook, a corporation without a shopfront or employees in Australia, 'carries on business' in Australia, at least for the purposes of the *Privacy Act 1988* (Cth) (***Privacy Act***).

Background

As any astute user of the internet would know, Meta provides users globally with access to their various social media platforms, including Facebook. In order to create a Facebook account, users input personal information including their name, age, email address or, from 2015, their telephone number. This account can then be used to connect with other users and build an online social network. Users may also find themselves inputting further personal information into the platform, including data relating to a person's hometown, educational history, work experience, sexual orientation, relationship status, occupation, political and religious views, interests and photographs. Facebook then monetises this personal information in the form of advertising revenue, including targeted advertisements, which may account for the occasional feeling that your phone is listening to you.

It is alleged that between 12 March 2014 and 1 May 2015, Facebook released users' personal information to a third party application called '*This is Your Digital Life*'. Approximately 50 Australians installed the application and permitted access to their personal information. However, through the use of Facebook's social network and the connections of those 50 or so people, the application was able to obtain personal information (and in some cases sensitive information) from approximately 311,127 Australian Facebook users. The application then on sold the information to political consulting firm Cambridge Analytica Ltd, where it is alleged the personal information was at risk of being used for political profiling.

Key Takeaways

- The Privacy Act specifically envisioned that it could be possible to carry on business in Australia without having a physical presence in Australia.
- As such, the decision of the Full Court indicates the court is willing to construe the legislation in a way that makes it possible for the Commissioner to bring cases in Australia where the 'carrying on business' might seem tenuous on first glance.
- It is possible that the decision of the Full Court may impact other foreign corporations which install cookies on Australian devices. Nonetheless, because the applicable test is one of fact finding, the exposure risk will depend on the circumstances in each individual case.
- The Full Court has indicated, at least in respect of privacy matters, a reluctance to apply case law which considered historical technologies to a modern landscape in circumstances where present day technology was not in existence in its relevant form at the time of the decision.

In proceedings brought by the Australian Information Commissioner, the Commissioner alleged that:

1. Facebook disclosed users' personal information for a purpose other than that for which it was collected, in breach of the Australian Privacy Principle (**APP**) 6;
2. Facebook failed to take reasonable steps to protect the users' personal information from unauthorised disclosure in breach of APP 11.1(b); and
3. these breaches amounted to serious and/or repeated interferences with the privacy of the users, in contravention of s 13G of the *Privacy Act*.

As a preliminary question, the Commissioner was required to establish a *prima facie* case that Facebook:

1. carried on business in Australia under s 5B(3)(b); and
2. collected or held personal information in Australia under s 5B(3)(c).

The matter proceeded before Justice Thawley at first instance.

1 [2022] FCAFC 9.

Judgment at First Instance

The term 'carrying on business' for the purpose of the *Privacy Act* may have different meanings depending on context.[2] In order to determine whether a company is 'carrying on business' in Australia, there needs to be a sufficient connection to the country. Simply transacting in Australia is not sufficient to establish that a company is carrying on business. That being said, it is possible that a company which does conduct business in Australia, but does not have a physical presence in Australia, may be found to carry on their business here.[3] The court is invited to engage in a fact finding expedition in order to determine whether a sufficient connection is established in each circumstance.

In their submissions, the Commissioner placed significant emphasis on the Explanatory Memorandum to the *Privacy Amendment (Enhancing Privacy Protections) Bill 2012* (Cth), which amended s 5B of the *Privacy Act*. The Explanatory Memorandum states, in its relevant parts:

> The collection of personal information 'in Australia' under paragraph 5B(3)(c) includes the collection of personal information from an individual who is physically within the borders of Australia or an external territory, by an overseas entity.
>
> For example, a collection of personal information is taken to have occurred 'in Australia' where an individual is physically located in Australia or an external Territory, and the information is collected from that individual via a website, and the website is hosted outside of Australia, and owned by a foreign company that is based outside of Australia and that is not incorporated in Australia. It is intended that, for the operation of paragraphs 5B(3)(b) and (c) of the *Privacy Act*, entities such as those described above who have an online presence (but no physical presence in Australia), and collect personal information from people who are physically in Australia, carry on a 'business in Australia or an external territory'.

The Commissioner submitted that, in installing, operating and removing cookies from Australian users' devices, Facebook was both carrying on its business in Australia (for the purpose of s 5B(3)(b)) but also collecting and holding personal information (for the purpose of s 5B(3)(c)). Facebook's 2013 Data Use Policy described cookies as:

> Small pieces of data that are stored on your computer, mobile phone or other device. ... We use technologies like cookies, pixels, and local storage... to provide and understand a range of products and services.

In response, Facebook submitted the process of installing, operating and removing cookies was not performed by any person in Australia. Instead, on their submission, the cookies were uploaded overseas and then later downloaded in Australia by Facebook users. To this point, Facebook relied on Justice Barrett's judgement in *Campbell v Gebo Investments (Labuan) Ltd*, where His Honour opined:

> Advances in technology making it possible for material uploaded on to the Internet in some place unknown to be accessed with ease by anyone in Australia with Internet facilities who wishes (or chances) to access it cannot be seen having carried with them any alteration of principles as to the place carrying on business developed at times when such communication was unknown. [...]
>
> Unless there is evidence of activities in Australia of placing material on the Internet or processing and dealing with inquiries or applications received by Internet, the question whether (a corporation) carried on business in Australia must be addressed by reference to the elements of the evidence that go beyond internet solicitation.[4]

On balance, Justice Thawley was satisfied that the Commissioner had established that it was arguable that some of the data processing activities carried on by Facebook, including the installation of cookies onto users' devices, occurred in Australia.[5] His Honour found this to be so even though the evidence did not establish that any employee of Facebook was physically located in Australia. His Honour was also satisfied that Facebook directly collected and stored information through the use of cookies on users' devices within Australia for the purpose of s 5B(3)(c).

Appeal

The Full Court upheld the decision of Justice Thawley, reasoning:

> The acts occurring in Australia, on Australian users' devices, being the installation and deployment of cookies to collect information and help deliver targeted advertising, and the management of the Graph API to facilitate the collection of even more data may lack an intrinsic commercial character in and of themselves, but they are integral to the commercial pursuits of Facebook.[6]

The Full Court considered that the use of cookies by Facebook is 'one of the things which makes Facebook work'.[7]

The Full Court considered the concept of carrying on business in Australia must reflect the type of business being conducted. The Full Court also observed that the cases which have historically discussed the meaning of 'carrying on business' were not reflective of the current and emerging technological advances in business.[8]

The Full Court also upheld that the collection of users' personal information through the use of cookies installed on their devices occurred within Australia for the purposes of s 5B(3)(c).[9]

2 *Tiger Yacht Management Ltd v Morris* (2019) 268 FCR 548, [50].
3 *Anchorage Capital Pty Ltd v ACPA Pty Ltd* (2018) 259 FCR 514, [99].
4 (2005) 190 FLR 209, [33]-[34].
5 *Australian Information Commissioner v Facebook Inc (No 2)* [2020] FCA 1307, [137] (Thawley J).
6 *Facebook Inc v Australian Information Commissioner* [2022] FCAFC 9, [9] (Allsop CJ).
7 Ibid [43] (Perram J).
8 Ibid [74] (Perram J).
9 Ibid [143] (Perram J).

Digital Platform Services Inquiry – March 2022 Interim Report

Tara Taylor, McCullough Robertson, comments on the ACCC's March 2022 interim report into digital platform services.

As part of its broader inquiry into digital platforms, in late April 2022 the Australian Competition and Consumer Commission (**ACCC**) released its fourth Interim Report (**Interim Report**) which examines potential competition and consumer issues in Australian general online retail markets. With the COVID pandemic leading to an increase of almost 31% in online spending in 2020-2021 compared to 2019-2020[1], it's not surprising that the ACCC has focused its inquiry on online markets that facilitate transactions between third-party sellers and consumers through a common platform (such as Amazon, eBay, Catch and Kogan) (**online marketplaces**).

In contrast to other jurisdictions which have claimed that Amazon dominates online marketplaces, the ACCC considers that no online marketplace currently possesses market dominance in Australia. However, due to their multi-sided nature and unique business operations, the ACCC has raised concerns that if an online marketplace attains substantial market power, it may adopt a gatekeeper position and in turn stifle competition in Australia. This article outlines the operations of online marketplaces in Australia, the key issues raised by the ACCC and its proposed solutions to protect consumers and ensure online marketplaces remain competitive.

Key Takeaway

- The Interim Report aligns with the ACCC's broader approach to digital platform regulation. Unlike social media platforms or search engines (which have also to significant examination by the ACCC), the ACCC considers that no one online retail marketplace currently has substantial market power in Australia. However, to address competition concerns that may arise if the Australian market 'tips' and to more generally protect Australian consumers, the ACCC has proposed a series of reforms which if implemented will place increased obligations on online retail marketplaces operating in the Australian market.

Online marketplaces in Australia

Online marketplaces play an important role in connecting Australian consumers and businesses and fostering trust and confidence in the digital economy. Unlike the United Kingdom and United States, the ACCC considers that there is currently no dominant firm in the Australian online retail marketplace. However, the ACCC has noted that the Australian market is dynamic and that there is potential for the market to 'tip' in favour of a single dominant marketplace.

In the Interim Report, the ACCC identified the following features as being key to scrutiny and likely to cause the Australian market to 'tip':

- **(Cross side network effects)** the more sellers on an online retail marketplace, the more attractive it is to consumers and the more consumers, the more attractive the marketplace is to sellers;
- **(Same-side network effects)** the more consumers attracted to an online retail marketplace, the greater the ability of the platform to collect data regarding consumer preferences. The more this data can be used to improve the matching of consumer preferences to products, the more attractive the online retail marketplace becomes to other consumers; and
- **(Limited bargaining power of other sellers)** when moving away from an online marketplace, sellers may face various learning and implementation costs. If a seller seeks to create their own website or physical store, they will also face establishment costs. These costs mean that sellers have limited bargaining power when dealing with large online market places – including in relation to the fees paid to the online marketplace operator.

Achieving market power is not in itself a competition concern and may in fact be evidence of effective competition in a highly concentrated market. However, the ACCC has indicated that where 'tipping' leads to a dominant retail marketplace behaving anti-competitively or reducing the benefits that consumers and sellers might otherwise gain from competition, it will intervene.

Key issues raised by ACCC

Like other digital platform services, the growth of hybrid marketplaces presents a unique regulatory challenge due to the greater consumer choice these platforms afford and conversely the competition concerns they raise. For example, despite providing a low-cost way for sellers to enter the market and increasing consumer choice, where an online marketplace sells its own goods in competition with a third party, competing incentives may exist to prevent or inhibit third party sellers from competing on their merits. The ACCC has recognised such issues and considers that hybrid marketplaces should inform consumers and third-party sellers about the factors that influence how prominently products are displayed (e.g. when favourable treatment is being provided to the online marketplace's own products) especially where those reasons appear less relevant to a consumer.

In addition to the above, some other issues raised by the ACCC regarding online marketplaces include:

- **(Data control)** the data practices of online marketplaces are often misaligned with consumer preferences to limit the collection and use of their data; and

1 Australia Post, Inside Australian Online Shopping – eCommerce Industry Report August 2021, 27 August 2021, p4.

- **(Lack of dispute resolution mechanisms)** consumers may have limited recourse to dispute resolution mechanisms outside of the policies of an online retail marketplace which in the event of a dispute, may act as the forum, adjudicator and fact-finding body.

Proposed solutions

To provide consumers with greater protections when purchasing products online and to ensure that smaller firms are able to effectively compete in online retail marketplaces, the ACCC has expressed its support for solutions identified in previous reports and also proposed new solutions to deal with the challenges posed by online retail marketplaces. The ACCC also noted, by way of example, the success of the Product Safety Pledge which has been entered into by some online marketplaces.

These solutions include:

- **(Introducing a prohibition on unfair trading practices)** the ACCC reiterated its support to introduce a prohibition on unfair trading practices to cover harmful conduct which falls outside of existing provisions. If introduced, this prohibition may address concerns regarding the data collection and use by online marketplaces and 'nudges' where a user is encouraged to take action that may not be in their best interests;
- **(Making unfair contract terms illegal and introducing civil pecuniary penalties)** the ACCC also continues to support making unfair contract terms illegal (as opposed to just voidable) and argues that this would act as an effective deterrent to online retail marketplaces when using any unfair contract terms in small business agreements;
- **(Internal dispute resolution mechanisms and ombudsman scheme)** the ACCC has supported its recommendation in the 2019 Digital Platforms Inquiry Final Report to introduce an ombudsman scheme and has suggested that this scheme be developed in a way that would also assist sellers resolve disputes with consumers and online market places. The ACCC proposes that this will assist address some of the consequences that arise from the limited bargaining power of sellers who operate on hybrid marketplaces; and
- **(Introducing a general safety provision)** the introduction of a general safety provision would require businesses to supply safe products to the Australian market. This proposal is being considered by the Australian Government's Department of the Treasury and the ACCC has indicated it should be carefully considered to ensure that any burden placed on online marketplaces is appropriately balanced.

How to Treat an Angry Tweet – the Dutton v Bazzi Appeal

Kevin Lynch and **Jade Tyrrell,** Johnson Winter & Slattery, consider the Full Federal Court's decision in Peter Dutton's defamation proceedings.

The Full Court's Decision

The Full Court of the Federal Court has allowed an appeal, setting aside a judgment entered in favour of the Hon. Peter Dutton MP in which it was found that a 'tweet' conveyed the defamatory imputation that "Mr Dutton excuses rape" (see *Dutton v Bazzi* [2021] FCA 1474), and ordered that the proceeding be dismissed.[1]

In dismissing the proceeding, the Full Court overturned the trial judge's finding that a defamatory imputation had arisen in the tweet published by Mr Bazzi which had included an extract and link to an article by *The Guardian*.

The content of posts in the form of tweets must be read in the context of the tweet, "as a whole"[2] to ascertain the meaning conveyed. This means that a 'bare tweet' which shares an extract from a linked article as part of that tweet should not be separated from that extract when determining whether a particular defamatory imputation is conveyed.

Background

The primary judge was required to determine whether an ordinary reasonable reader would understand that the tweet conveyed the defamatory imputation. White J found that this was the case and that Mr Dutton was entitled to damages in the sum of $35,825 (including interest) Mr Bazzi appealed that decision.

In the tweet itself, Mr Bazzi had shared the article from *The Guardian* with the text "*Peter Dutton is a rape apologist*", and it appeared on Twitter as follows:

Key Findings

- The primary judge failed to take an "impressionistic approach" and placed undue focus on dictionary definitions instead of properly considering the six-word statement in the tweet in the context of the tweet as a whole.[3]
- The primary judge erred in his reasoning process as he did not explain in his reasons how the reader would understand the whole of the tweet (or any part of it) to convey the imputation, particularly given his analysis of the meaning of the word "apologist" to mean a defender of something.[4]

Mr Dutton at first instance had pleaded and relied on four imputations which he said arose from the tweet, being that Mr Dutton:

a) condones rape;

b) excuses rape;

c) condones the rape of women; and

d) excuses the rape of women.

It was the second imputation above (that "Mr Dutton excuses rape") which White J found was conveyed by the tweet and which was before the Full Court of the Federal Court for consideration on appeal.

Outcome

The Full Court of the Federal Court, comprised of Rares and Rangiah JJ (in a joint judgment), and Wigney J (agreeing, in a separate judgment) allowed the appeal and dismissed the proceeding.

The only issue the Full Court was required to consider and determine in the appeal was whether the primary judge erred in finding that Mr Bazzi's tweet conveyed the particular imputation. There was no dispute as to correctness of the primary judge's identification of the principles to be applied to determine whether a publication conveyed a particular defamatory meaning or imputation.[5]

1 *Bazzi v Dutton* [2022] FCAFC 84.

2 [33] per Rares and Rangiah JJ; [63], [71] per Wigney J.1

3 [71] per Wigney J.

4 [40] per Rares and Rangiah JJ.

5 [4] per Rares and Rangiah JJ, citing the judgment of the judgment of Lord Kerr of Tonaghmore JSC in *Stocker v Stocker* [2020] AC 593, and [56] per Wigney J.

Rares and Rangiah JJ rejected Mr Dutton's submission that Mr Bazzi's six-word statement in the tweet conveyed the imputation independently of the content of the tweet when read as a whole.[6] Rares and Rangiah JJ endorsed[7] a recent UK social media case and stated:

> *"...it is the general impression created in the mind of the ordinary reasonable reader of a publication that determines whether it conveys one or more imputations of and concerning a claimant....in considering what a tweet conveys, Lord Kerr JSC cautioned against an elaborate analysis of the tweet or parsing of its content, because the medium has the nature of a conversation in which participants ordinarily correspond without using carefully chosen expressions."*[8]

In addition to the Key Findings and the matters outlined above, their Honours found that:

- While it is open to a claimant to plead that an imputation arises from part of a publication if a separate meaning is conveyed, the general or broad impression of the tweet must be considered, and the natural and ordinary meaning of the tweet by Mr Bazzi would not give the impression to the reader that it conveyed two messages.[9]
- The primary judge was wrong to have downplayed the balance of the tweet (being the extract from the linked article), and dissect and segregate parts of the tweet, as Twitter users, being users of a conversational medium, would not do so. The ordinary reasonable reader would instead have read Mr Bazzi's tweet with regard to the incorporated article extract.[10]

As such, taking the tweet as a whole in its context, it was not accepted by their Honours that the tweet would have conveyed the imputation to the ordinary reasonable reader.[11] Part of that stems from the fact that Mr Bazzi's tweet was something of a *non sequitur* when read with the article extract. Wigney J described an "element of disjunct or disconnect" between the six-word statement in the tweet and the article extract, which made the tweet "confounding" and the meaning "obscure".[12]

An echo of *Hockey v Fairfax Media Publications*

Mr Dutton is not the first Australian Cabinet Minister to commence defamation proceedings in relation to tweets in which the defendant published a handful of words concerning a politician, in conjunction with an article hyperlink. In *Hockey v Fairfax Media Publications Pty Limited* the Federal Court of Australia considered (among other matters) tweets concerning Mr Joe Hockey, the then Federal Treasurer. One of the issues to be determined was whether, for the tweets in which *The Age* (as the publisher of the tweets) had provided an accompanying hyperlink to *The Age*'s own article, the Court should take into account the articles linked in the tweets or whether the defamatory meaning was to be determined by reference only to the text of the tweets themselves (i.e. the 'bare tweet'). The first of these tweets involved a truncated hyperlink and the second contained a "view on web" hyperlink. That case also involved his Honour, White J, as trial judge, who considered that the meaning conveyed by those tweets may be determined without reference to the article to which the tweet links, as some may read the bare tweet without accessing the article.[13]

Whilst the presentation of the tweeted content with the truncated hyperlink to *The Age* article in *Hockey* appears to have differed from the way Mr Bazzi's tweet displayed an extract from *The Guardian* article, His Honour, White J was consistent in drawing a line between the words of the Twitter commentator and the linked article (in *Hockey*) and the extracted article (in *Dutton*).[14]

A parallel approach in Defamation Act Reforms

Bazzi v Dutton makes it clear that where an extract of an article is published as part of a tweet so that it is to be read with the tweet, one can reasonably expect that this requires a court to consider the tweet as a whole, including the material extracted from the linked article,[15] to determine the defamatory meaning or imputation.

This decision also highlights the role of platforms such as Twitter in public conversation and the nature of the medium, which involves users scrolling through content and reviewing tweets quickly to gain an impression.

The commencement of the Model Defamation Amendment Provisions on 1 July 2021 in a number of Australian jurisdictions has seen the statute recognise the operation of a link in the experience of an online reader, albeit in consideration of a defence rather than in assessing meaning. Section 31(5) of the *Defamation Act 2005* (NSW) now provides that material on which an opinion is based may include material which is "*accessible from a reference, link or other access point included in the matter (for example, a hyperlink on a webpage)*"[16].

---

6 [45] per Rares and Rangiah JJ.

7 [47] per Rares and Rangiah JJ.

8 Citing *Stocker v Stocker* [2020] AC 593 at 606 [43].

9 [46] – [48] per Rares and Rangiah JJ.

10 [60], [63] per Wigney J.

11 [50] per Rares and Rangiah JJ and [77], [79] per Wigney J.

12 [75] per Wigney J.

13 *Hockey v Fairfax Media Publications Pty Limited* [2015] FCA 652 at [207].

14 *Hockey v Fairfax Media Publications Pty Limited* [2015] FCA 652 at [213]. The judge found that a third Twitter matter complained of tendered in the case "in conjunction with" a linked copy of the article as it appeared on The Age's website, the ordinary reasonable reader would not have understood it to mean that Mr Hockey was engaging in corrupt conduct, as he claimed. This was because the reader's initial understanding on reading the summary in the tweet itself (i.e. the imputation that Mr Hockey was engaging in corrupt conduct) would have been dispelled when the reader read the accompanying article.

15 [63] per Wigney J.

16 *Defamation Act 2005* (NSW), section 31(5)(iii).

Source Confidentiality Under Siege: How Law Enforcement Powers Threaten Journalists' Ethical Obligations

Adam Lukacs, University of Queensland, in his CAMLA Essay Competition winning piece, comments on the legislative framework protecting the confidentiality of journalists' sources.

I Introduction

The media are regarded as the 'eyes and ears' of the public.[1] In the course of acting as a public watchdog and gathering news, journalists occasionally guarantee anonymity to sources to preclude them from being subject to retribution for exposing matters of public interest to the media.[2] However, journalists enjoy limited protections for their sources under Australian law, and such protections face unique challenges in the context of metadata retention and national security regimes.[3] Relevantly, the vulnerability of source confidentiality was highlighted by the Australian Federal Police's raids on the home of Annika Smethurst and the Australian Broadcasting Corporation's Sydney headquarters in June 2019, which arose out of Smethurst's reporting on a proposal to expand federal surveillance powers.[4] One aim of the raid had been to identify the anonymous source who had provided Smethurst with classified information concerning the proposal. This essay will argue that police powers of search and seizure pose a significant threat to journalistic source confidentiality, specifically with respect to laws that provide a framework for data surveillance. The protections afforded to journalists and their sources under these regimes are weak, and such laws therefore represent a grave intrusion on journalists' ethical obligations when less intrusive alternatives are available. In this respect, the journalists' ethical obligations with respect to source confidentiality will first be discussed, followed by an assessment of the legal regimes which threaten source confidentiality.

Metadata retention laws, Journalist Information Warrants and the industry assistance scheme will be encompassed in this discussion. Finally, how these regimes undermine shield laws and how shield laws could potentially be reformed to better protect journalists and their sources in this context will also be explained.

II Journalistic Ethical Obligations

Source confidentiality is a core ethical obligation for journalists and a central tenet of press freedom.[5] Failure to provide source confidentiality would risk deterring sources from assisting the press in informing the public on matters of public interest.[6] A journalist's obligation to preserve the confidentiality of a source where they have agreed to do so is found, *inter alia*, in Clause 3 of the Media, Entertainment & Arts Alliance Journalist Code of Ethics.[7] Clause 3 relevantly provides that "where confidences are accepted, respect them in all circumstances".[8] Despite the ethical breach that revealing a source's identity would entail and the negative repercussions that would follow from this,[9] such as exposing the source to danger and eroding the trust between journalists and their sources,[10] Australian law provides minimal protection for journalists who face such a demand.[11] Journalists' ethical codes have no legal status and courts have consistently refused to recognise the existence of any 'journalists' privilege' protecting a journalist from disclosing their sources.[12] A journalist will be required to reveal a source in court proceedings if it is "necessary in the interests of justice"[13]

---

1 *Attorney General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109, 183 (Sir Donaldson MR).

2 Sanette Nel, 'Journalistic Privilege: Does it Merit Legal Protection?' (2005) 38(1) *Comparative and International Law Journal of South Africa* 99, 100.

3 Sal Humphreys and Melissa de Zwart, 'Data Retention, Journalist Freedoms and Whistleblowers' (2007) 165(1) *Media International Australia* 103, 103.

4 Rebecca Ananian-Welsh, '*Smethurst v Commissioner of Police* and the Unlawful Seizure of Journalists' Private Information' (2020) 25 *Media & Arts Law Review* 60, 60, 61. See *Smethurst v Commissioner of Police* (2020) 376 ALR 575; *Australian Broadcasting Corporation v Kane* (2020) 377 ALR 711 ('*Kane*').

5 Rebecca Ananian-Welsh, 'Journalistic Confidentiality in an Age of Data Surveillance' (2019) 41(2) *Australian Journalism Review* 225, 225 ('Journalistic Confidentiality'); *Mahon Tribunal v Keena and Kennedy* [2009] IESC 64 [23] (Fennelly J). See also Human Rights Committee, *General Comment No 34: Article 19, Freedoms of Opinion and Expression*, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011) [13], [19], [45].

6 *Goodwin v United Kingdom* (1996) 22 EHRR 123 [39]; Joseph Fernandez, 'Pass the Source – Journalism's Confidentiality Bane in the Face of Legislative Onslaughts' (2017) 27(2) *Asia Pacific Media Educator* 202, 203.

7 Mark Pearson, *The Journalist's Guide to Media Law: A Handbook for Communicators in a Digital World* (Taylor & Francis Group, 6th ed, 2019) 318.

8 'MEAA Journalist Code of Ethics', *Media, Entertainment & Arts Alliance* (Web Page) <https://www.meaa.org/meaa-media/code-of-ethics/>.

9 Lawrence McNamara and Sam McIntosh, 'Confidential Sources and the Legal Rights of Journalists: Re-Thinking Australian Approaches to Law Reform' (2010) 32(1) *Australian Journalism Review* 81, 81–82.

10 Media, Entertainment & Arts Alliance (MEAA), Submission No 90 to Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the Telecommunications (Interception and Access Amendment (Data Retention) Bill 2014* (19 January 2015) 4 ('MEAA Submission'); *Kane* (n 4) 720 [36]–[37], 723 [46] (Abraham J); Pearson (n 7) 318.

11 McNamara and McIntosh (n 9) 81.

12 *McGuinness v Attorney-General (Vic)* (1940) 63 CLR 73, 87 (Rich J); *Harvey and McManus v County Court of Victoria* (2006) 164 A Crim R 62, 79–80 [90] (Hollingworth J); *R v McManus and Harvey* [2007] VCC 619 [34]–[35] (Chief Judge Rozenes); *Kane* (n 4) 755 [197] (Abraham J); *Liu v The Age Company Ltd & Ors* (2016) 92 NSWLR 679, 706 [123] (McColl JA); *Re Evening News* (1880) 1 LR (NSW) 211, 240 (Martin CJ). See Joseph Fernandez, 'Journalists' Confidential Sources: Reform Lessons from Recent Australian Shield Law Cases' (2014) 20(1) *Pacific Journalism Review* 117, 129.

as there is a paramount public interest in securing the administration of justice which no undertaking of confidentiality can override.[14] Despite the potential consequences for refusing to disclose sources, journalists have stalwartly adhered to this ethical principle,[15] even with the prospect of severe fines or imprisonment.[16] Indeed, this is unsurprising as sources remain the "wellspring of journalists' work" — source confidentiality encourages the free flow of information in a democratic society because confidential disclosures provide vital information that supports public interest journalism.[17] However, despite widespread recognition of the crucial link between press freedom and source confidentiality,[18] and journalists' ardent commitment to source protection, the capacity of journalists to protect their sources is fragile in light of technological developments and national security laws that now pose a threat to guaranteeing source anonymity.[19]

III Vulnerability of Source Confidentiality

A Law Enforcement Powers

Government search, seizure and surveillance powers vastly expanded in the aftermath of 9/11,[20] with 75 pieces of counter-terrorism legislation being enacted since 2001.[21] While police raids such as the one on Smethurst's home and the ABC present a clear threat to source confidentiality, federal covert data surveillance schemes represent a far more insidious danger.[22]

1. *Data Retention*

As amended in 2015, the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA**) implements a national scheme for mandatory data retention, obligating all telecommunications providers in Australia to retain customer metadata for at least two years.[23] There is no definition of 'metadata' in the legislation, but such providers are required to retain, among other things, information relating to the time, date and location of communications passing over their services.[24] Such data consists of information about a communication or parties to a communication, as distinct from the content or substance of that communication, which is inaccessible except under a warrant.[25] This data can nevertheless reveal significant identifying and personal information about one's contacts, communications, activities and whereabouts,[26] and is accessible without a warrant by ASIO if disclosure would be in connection with the performance by ASIO of its functions[27] and by other law enforcement agencies if it is 'reasonably necessary for the enforcement of the criminal law'.[28] Such data not only captures the communications between a journalist and a source but also the fact that information has passed between them and the details of when, where and how they communicated.[29] Law enforcement agencies can triangulate this information in such a way to reveal the identity of a journalist's sources,[30] demonstrating the threat that these law enforcement powers pose to source confidentiality as such powers potentially allow law enforcement to frustrate journalists' efforts to maintain source confidentiality by examining their metadata.

2. *Journalist Information Warrants*

However, because accessing journalists' metadata may reveal their confidential sources, the TIA includes a Journalist Information Warrant (**JIW**) scheme.[31] This allows a journalist's metadata to be accessed for the purpose of identifying a confidential source if the public interest

13 *John Fairfax & Sons Ltd v Cojuangco* (1988) 165 CLR 346, 354–355 (Mason CJ, Wilson, Deane, Toohey and Gaudron JJ).

14 *Nicholls v Director of Public Prosecutions (SA)* (1993) 61 SASR 31, 41 (Legoe ACJ), 51 (Perry J); *Independent Commission Against Crime and Corruption v Cornwall* (1993) 38 NSWLR 207, 234 (Abadee J); *Von Doussa v Owens (No 3)* (1982) 31 SASR 116, 117 (King CJ); *Re Buchanan* (1964) 65 SR (NSW) 9. See also *X Ltd v Morgan-Grampian Publishers* [1991] 1 AC 1, 48 (Lord Bridge).

15 National Press Club, 'NPC Statement on the AFP Raids', *National Press Club of Australia* (Web Page, 5 June 2019) <https://www.npc.org.au/article/freedom-of-the-press/2019/75-npc-statement-on-the-afp-raids>; MEAA Submission (n 10) 4. See Wendy Bacon and Chris Nash, 'Confidential Sources and the Public Right to Know' (1999) 21(2) *Australian Journalism Review* 1, 1–2.

16 See, eg, *R v Kessing* (2008) 73 NSWLR 22, 35 [57] (Bell JA); *R v Barrass* (unreported, District Court of Western Australia, Judge Kennedy, 7 August 1990); *R v Budd* (unreported, Supreme Court of Queensland, Dowsett J, 20 March 1993).

17 Des Butler and Sharon Rodrick, *Australian Media Law* (5th ed, Thomson Reuters, 2015) 689; *Ashby v Commonwealth of Australia (No 2)* [2012] FCA 766 [18] (Rares J) ('*Ashby*'); *McKenzie and Baker v Magistrates' Court of Victoria and Leckenby* [2013] VSCA 81 [3] (Harper JA).

18 Human Rights Committee (n 5) [2]–[3].

19 Moira Paterson, 'The Public Privacy Conundrum – Anonymity and the Law in an Era of Mass Surveillance' in Johan Lindberg and Denis Muller (eds), *In the Name of Security – Secrecy, Surveillance and Journalism* (Anthem Press, 2018) 15, 15.

20 Ananian-Welsh, Journalistic Confidentiality (n 5) 226.

21 George Williams and Kieran Hardy, Submission No 11 to Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press* (26 July 2019) 1 ('Williams and Hardy Submission').

22 Ananian-Welsh, Journalistic Confidentiality (n 5) 226.

23 Ibid; *Telecommunications (Interception and Access) Act 1979* (Cth) ss 187A, 187AA, 187C ('TIA').

24 TIA (n 23) s 187AA; Williams and Hardy Submission (n 21) 7.

25 TIA (n 23) ss 7, 108, 172; Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (Report, 27 February 2015) 12 [2.17].

26 Williams and Hardy Submission (n 21) 7. See also *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Kärntner Landesregierung* (Court of Justice of the European Union, C-293/12 and C-594/12, 8 April 2014) [27].

27 TIA (n 23) ss 174–175.

28 Ibid ss 110A, 177–180. See also Centre for Media Transition, Submission No 31 to Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press* (31 July 2019) 4 ('Media Transition Submission').

29 MEAA Submission (n 10) 6; Ananian-Welsh, Journalistic Confidentiality (n 5) 227; Paterson (n 19) 17.

30 See, eg, *F v Crime and Corruption Commission* [2021] QCA 244 [4] (Mullins JA).

31 Mark Pearson and Joseph M. Fernandez, 'Surveillance and National Security 'Hyper Legislation' – Calibrating Restraints on Rights with a Freedom of Expression Threshold' in Johan Lidberg and Denis Muller (eds), *In the Name of Security – Secrecy, Surveillance and Journalism* (Anthem Press, 2018) 51, 66.

in issuing the warrant outweighs the public interest in protecting the journalist's sources.[32] The public interest requirement involves considerations of privacy and whether reasonable attempts have been made to obtain the information otherwise.[33]

'Source' is defined narrowly in the TIA to only capture journalists 'working in a professional capacity'.[34] A JIW is therefore not required to access metadata to identify a source who provides information to a non-professional journalist, meaning that the JIW scheme only applies to some journalist-source interactions and confers no protection to journalistic confidentiality outside of 'professional' journalism.[35] This represents a problematic intrusion on journalists' ethical obligations, as the definition of 'source' allows law enforcement to access the metadata of an individual engaged in legitimate and good faith journalism, who may otherwise not be a 'professional journalist', to uncover their sources without a JIW.[36]

Agencies may seek a JIW from an 'issuing authority',[37] which must only issue a JIW if it is satisfied that the warrant is for a specified law enforcement purpose.[38] These purposes include enforcing the criminal law, finding a missing person, enforcing laws that impose financial penalties, protecting the public revenue or for the investigation of a serious offence punishable by at least three years' imprisonment.[39] While this 'purpose test' provides some limit on the scope of JIWs, this requirement may be easily fulfilled in the context of Australia's secrecy-based offences.[40] Under these laws, specifically espionage offences that criminalise a wide range of conduct pertaining to the handling and communication of classified and national security information,[41] a JIW could be obtained to investigate the potential leaking of classified information before determining whether the source was covered by whistleblower protections.[42]

The JIW regime is therefore a minor obstacle to law enforcement agencies accessing information for the direct purpose of identifying a journalist's confidential source. Further, journalists may be subject to criminal penalties under these laws for merely receiving or possessing sensitive information, even prior to publication.[43] This gives rise to the risk that the JIW regime may be employed to access a journalist's metadata to prevent the disclosure of information leaked to journalists or to discover the source of a leak.[44] A promise of confidentiality made by a journalist to a particular source therefore becomes meaningless where a relatively easily-obtained JIW entitles law enforcement to identify that source,[45] thus demonstrating the intrusion on journalists' ethical obligations that these law enforcement powers represent.

Further, journalists cannot contest JIWs because of secrecy provisions that render the revelation of the existence of a JIW application or an application's result a crime,[46] meaning that a journalist whose metadata is being targeted will not be informed of this.[47] While a targeted media organisation can have no input into the application for a JIW, an issuing authority will be assisted by submissions made by the 'Public Interest Advocate' (**PIA**) with respect to the public interest test.[48] However, the PIA does not represent the interests of journalists and is insufficiently directed towards protecting the freedom of the press as opposed to other public interests, such as national security.[49] The coalescence of the perceived inadequacy of the public interest and purpose tests, the PIA's lack of representing journalists' interests, scant oversight and there being no independent assessment of a JIW application by a superior court judge[50] has prompted calls for media organisations to be notified of the existence of JIWs in relation to them and for JIWs to be issued by judges in contested hearings.[51] There is a significant threat to source confidentiality posed by the capacity for law enforcement agencies to covertly access journalists' data for the express purpose of source identification, which

32 TIA (n 23) ss 180J, 180L, 180T; Williams and Hardy Submission (n 21) 7; Rebecca Ananian-Welsh et al, Submission No 17 to Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press* (26 July 2019) 10 ('Ananian-Welsh Submission').

33 TIA (n 23) s 180T(2)(b); Paterson (n 19) 20.

34 TIA (n 23) s 5(1) (definition of 'source').

35 Ananian-Welsh, Journalistic Confidentiality (n 5) 228.

36 Ibid 235.

37 TIA (n 23) ss 5(1), 6DB–6DC.

38 Ananian-Welsh, Journalistic Confidentiality (n 5) 228.

39 TIA (n 23) ss 178–180(4), 180T(2)(a); Ibid.

40 Ananian-Welsh, Journalistic Confidentiality (n 5) 228.

41 See, eg, *Criminal Code Act 1995* (Cth) ss 91.1–92A; *Australian Security Intelligence Organisation Act 1979* (Cth) ss 18(2), 18A(1), 18B(1), 35P, 92(1); *Defence Act 1903* (Cth) s 73A; *Office of National Intelligence Act 2018* (Cth) ss 42, 45; *Crimes Act 1914* (Cth) ss 3ZZHA, 15HK; *Intelligence Services Act 2001* (Cth) ss 39–40M.

42 Ananian-Welsh, Journalistic Confidentiality (n 5) 228.

43 Williams and Hardy Submission (n 21) 9.

44 Ibid 9–10.

45 Nel (n 3) 111.

46 TIA (n 23) s 182A; Williams and Hardy Submission (n 21) 7; Ananian-Welsh, Journalistic Confidentiality (n 5) 229.

47 Media Transition Submission (n 26) 5.

48 Ibid; TIA (n 28) s 180T(2)(b)(v).

49 Ananian-Welsh Submission (n 32) 11.

50 Media Transition Submission (n 28) 7.

51 Ibid 3; Williams and Hardy Submission (n 21) 7; Ananian-Welsh, Journalistic Confidentiality (n 5) 235.

means that journalists may no longer be able to confidently fulfil their ethical obligations when they have guaranteed a source confidentiality.[52] The excessive secrecy of the JIW process, ineffective protections available under the JIW regime and onerous penalties for secrecy offences suggests that the law has disproportionately moved in favour of competing public interests such as national security,[53] representing an unjustified intrusion on journalists' ethical obligations in the process.

3. *'Acts and Things'*

The introduction of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (**TOLAA**) compounds the threat posed to journalistic confidentiality presented by mandatory data retention.[54] The TOLAA created industry assistance and computer access schemes and expanded the scope of search and seizure warrants, allowing law enforcement agencies to access the content of communications and overcome the use of encryption.[55]

Under the industry assistance scheme, policing and intelligence agencies can request or compel communications providers[56] to do a broad range of 'acts and things' to: assist an agency in their objectives;[57] enforce the criminal law as it relates to a serious criminal offence punishable by three or more years' imprisonment; safeguard national security; and, matters ancillary to those objectives.[58] 'Acts and things' importantly encompasses agencies being able to request or compel providers to remove electronic protections applied to telecommunications, including encryption, meaning such providers can be required to decrypt encrypted communications.[59] Accessing the content of a communication requires a valid warrant[60] and any such requests under this scheme are approved on the basis that they are 'reasonable, proportionate, practicable and technically feasible'.[61] While agencies are prohibited from requiring providers to build a 'systemic weakness' or 'systemic vulnerability' into their carriage services or devices,[62] this does not prevent an agency from requiring a provider to target a *specific* service or device.[63] For example, the AFP could require a provider to break past the passcode on a journalist's smartphone or insert an eavesdropping capability into a journalist's Google Home device.[64] Accessing the retrieved data would require a warrant but would allow agencies to uncover confidential sources without engaging the JIW provisions, as they do not extend to requests to access information under the TOLAA.[65] The lack of acknowledgment of or protection for source confidentiality under the TOLAA raises serious concerns for the potential of a wide range of telecommunications actors to 'assist' government agencies in data surveillance, making it extremely difficult for journalists to ensure source confidentiality.[66]

This framework does not in and of itself operate as a data surveillance scheme, but presents a way for law enforcement agencies to circumvent encryption and other protection technologies used by journalists and their sources when communicating.[67] While access to journalists' data is not as simple under this scheme as under the TIA, journalists investigating national security matters or who interact with government sources may nevertheless be targeted under the TOLAA.[68] They may covertly be subject to orders to cause weaknesses to be built into their attempts to encrypt or protect their data and warrant-based access to their now decrypted communications,[69] exposing confidential communications between journalists and their sources.[70] The inclusion of maintaining the public interest in journalistic confidentiality as a necessary condition for the issuance of a TOLAA-related warrant authorising access to data would provide some degree of protection that does not currently exist, and thus make the TOLAA framework a somewhat more proportionate intrusion on journalists' ethical obligations.[71] However, in their present form, these laws pose a significant threat to source confidentiality because, to the extent that journalists use electronic devices or web-based accounts, they can offer no assurances of confidentiality to their

52 Ananian-Welsh, Journalistic Confidentiality (n 5) 226.

53 Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the Impact of the Exercise of Law Enforcement Powers on the Freedom of the Press* (Report, August 2020) 129 [3.306] ('PJCIS Report'); Media Transition Submission (n 28) 3.

54 Ananian-Welsh, Journalistic Confidentiality (n 5) 230.

55 Ibid.

56 *Telecommunications Act 1997* (Cth) s 317C.

57 Ibid ss 317A, 317B, 317G; Ananian-Welsh, Journalistic Confidentiality (n 5) 231.

58 *Telecommunications Act 1997* (Cth) ss 317(1)–(2), 317B.

59 Ibid ss 317E(1)(a), 317B; Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 38 [54]; Ananian-Welsh, Journalistic Confidentiality (n 5) 231.

60 *Telecommunications Act 1997* (Cth) s 317ZH.

61 Ibid ss 317JAA, 317JC, 317P, 317RA, 317V, 317ZAA.

62 Ibid s 317ZG.

63 Ibid s 317B.

64 Ibid ss 317E(1)(c), 317L(1), 317T(1); Ananian-Welsh, Journalistic Confidentiality (n 5) 232.

65 Ananian-Welsh, Journalistic Confidentiality (n 5) 232.

66 Ibid 231, 233, 236.

67 Ibid 234.

68 Ibid.

69 Ibid.

70 Alliance for Journalists' Freedom, Submission No 13 to Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press* (2019) 4.

71 Ananian-Welsh, Journalistic Confidentiality (n 5) 236.

sources.[72] This breadth of powers is coupled with minimal independent oversight or accountability mechanisms, further undermining the already scarce protections afforded to journalists and their sources,[73] demonstrating the disproportionate nature of this intrusion on journalists' ethical obligations.

B Shield Laws

The clearest protection for source confidentiality is found in 'shield laws', which operate in every Australian jurisdiction except Queensland.[74] Shield laws aim to ensure that a journalist or their employer are not compellable to disclose the identity of a confidential source in court.[75] Such laws aim to foster freedom of the press not by protecting journalists themselves, but their anonymous sources, and thereby are a legislative acknowledgement of the public interest in source confidentiality.[76] Despite this acknowledgment, the protection offered by shield laws is precarious.[77] A court may order that the laws' protections do not apply if it is satisfied that 'the public interest in the disclosure of evidence of the identity of the informant' outweighs any likely adverse effect of the disclosure on the source and outweighs the public interest in the communication of facts and opinion by the media and the ability of the media to access sources.[78]

Relevantly, federal shield laws do not extend to investigatory or non-curial processes.[79] As a consequence, most Australian law enforcement agencies are easily able to circumvent the object of shield laws by using search powers to investigate journalists' records and identify their confidential sources before legal proceedings have even commenced.[80] This is in contrast to the Victorian position where shield law protections apply to police investigations, preventing a document that would identify a journalist's confidential source from being accessed under a regular warrant.[81] The Victorian position is aligned with the legislative shield law framework of other countries such as the United Kingdom and New Zealand, with these frameworks recognising that source confidentiality is just as important in police investigations as curial proceedings.[82]

Because law enforcement in weaker shield law jurisdictions can coercively obtain documentary evidence during the investigatory stage of criminal proceedings, the need to seek disclosure in court proceedings is obviated, consequently eroding the utility of shield laws.[83] This was especially highlighted by the Smethurst raids, as the AFP had access to all material on Smethurst's phone – confidential or otherwise – with shield laws offering no protection due to their exclusive applicability to court proceedings. The rise of metadata interception also necessitates that journalists must assume their conversations with their sources could be intercepted, thus negating the intent of shield laws that recognise and protect journalist privilege because such laws are easily circumvented.[84] These weaknesses in shield laws risk 'chilling' public interest journalism because if journalists operate knowing that they can become the subject of an invasive search warrant and potential sources understand that confidences cannot be assured because of this, neither party will be willing to engage in such journalism.[85]

Insofar as they can be used to bypass the protection offered by shield laws, these law enforcement powers represent a significant threat to source confidentiality, and the effective protection of source confidentiality would require statutory reform.[86] Were shield laws to be extended to police investigations and brought in line with the position of Victoria and other jurisdictions that offer strong protections for source confidentiality like New Zealand and the UK (and if Queensland enacted shield laws of this nature), sources would not be left vulnerable to identification at early, often crucial, stages of an investigation.[87] This framework would offer a more robust and complete protection, ensuring shield laws fulfil their operative purpose: to encourage the free flow of information, which risks being undermined if journalists and their sources are inadequately protected.[88]

---

72 Alliance for Journalists' Freedom, *Press Freedom in Australia* (White Paper, May 2019) 13; Australian Lawyers Alliance, Submission No 5 to Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press* (24 July 2019) 7 [9].

73 Ananian-Welsh, Journalistic Confidentiality (n 5) 234.

74 See, eg, *Evidence Act 1995* (Cth) s 126K; *Evidence Act 1995* (NSW) s 126K; *Evidence Act 2008* (Vic) s 126K; *Evidence Act 2011* (ACT) s 126K; *Evidence Act 1906* (WA) s 201.

75 Ibid.

76 *Hancock Prospecting Pty Ltd v Hancock* [2013] WASC 290 [174] (Pritchard J); Explanatory Memorandum, Evidence Amendment (Journalists' Privilege) Bill 2011 (Cth) [1]; Pearson and Fernandez (n 31) 67–68.

77 See Hannah Ryan, 'The Half-Hearted Protection of Journalists' Sources: Judicial Interpretation of Australia's Shield Laws' (2014) 19 *Media and Arts Law Review* 325.

78 See, eg, *Evidence Act 1995* (Cth) ss 126K, 131A. PJCIS Report (n 53) 130 [3.305]; Joseph M. Fernandez and Mark Pearson, 'Shield Laws in Australia: Legal and Ethical Implications for Journalists and their Confidential Sources' (2015) 21(1) *Pacific Journalism Review* 61, 67; Patrick George, 'Free Speech and Protecting Journalists' Sources: Preliminary Discovery, the Newspaper Rule and the Evidence Act' (2017) 36(2) *Communications Law Bulletin* 24, 30.

79 *Kane* (n 4) 757 [204]–[205]; Stephen Odgers, *Uniform Evidence Law* (Thomson Reuters, 15th ed, 2020) 20.

80 Rebecca Ananian-Welsh and Joseph Orange, 'The Confidentiality of Journalists' Sources in Police Investigations: Privacy, Privilege and the Freedom of Political Communication' (2020) 94 *Australian Law Journal* 777, 789.

81 *Evidence Act 2008* (Vic) s 131A.

82 *Contempt of Court Act 1981* (UK) s 10; *Evidence Act 2006* (NZ) s 68.

83 McNamara and McIntosh (n 9) 89.

84 Media, Entertainment and Arts Alliance, Submission No 98 to Parliamentary Joint Committee on Intelligence and Security, *Inquiry into Potential Reforms of National Security Legislation* (2012) 7.

85 Anna Kretowicz, 'Reforming Australian Shield Laws' (Reform Briefing 2/2021, Press Freedom Policy Papers, The University of Queensland, 2021) 5.

86 Ananian-Welsh and Orange (n 80) 789. See, eg, New Zealand Law Commission, *Review of the Search and Surveillance Act 2012* (Report No 141, June 2017).

87 Kretowicz (n 85) 7.

88 *Ashby* (n 17) [18] (Rares J).

III Conclusion

It is uncontroversial that law enforcement and intelligence agencies require significant powers to undertake overt and covert investigations to uphold public safety.[89] However, the TIA and TOLAA create and facilitate frameworks of covert surveillance which encumber journalists in ensuring source confidentiality, thus undercutting their ethical obligations in the name of security.[90] The TIA, TOLAA and the JIW schemes all place considerable pressure on journalists attempting to protect their sources and undermine the object of shield laws. In that regard, the present state of law enforcement powers poses a significant threat to journalistic confidentiality and represent an unjustified intrusion on journalists' ethical obligations. Journalists' ethical obligations have no legal support, leaving journalists in the position of having to defy police and the courts in order to honour their ethical obligations. The abovementioned covert search and surveillance powers may mean that journalists cannot guarantee their sources anonymity from law enforcement.[91] While Australia has a strong tradition of public interest journalism, the effect of these law enforcement powers undermines the ability of the 'fourth estate' to scrutinise and hold accountable government institutions through public interest journalism which is indispensable to facilitating this scrutiny.[92] The fact that these powers allow law enforcement to clandestinely uncover sources or effectively coerce journalists into disclosing them demonstrates that such powers place source confidentiality under siege, when authorities would prefer the public to remain in the dark.[93]

89 Ananian-Welsh Submission (n 32) 2.
90 Ibid; Ananian-Welsh, Journalistic Confidentiality (n 5) 233.
91 Ananian-Welsh, Journalistic Confidentiality (n 5) 236).
92 Richard Murray, Rebecca Ananian-Welsh and Peter Greste, 'Journalism On Ice: The Effect on Public Interest Reporting of National Security Legislation in Australia' in T Workneh and P. Haridakis, *Counter-Terrorism Laws and Freedom of Expression: Global Perspectives* (Lexington Books, 2021).
93 National Press Club (n 15).

FIRST, DO NO HARM: The Serious Harm Threshold in Defamation Cases Involving Physician-Review Websites

Nadine Mattini, University of Sydney, in her piece that won the second prize is CAMLA's Essay Competition, writes about defamation cases involving physician-review websites and the harm that a negative review can have on a physician's reputation in light of the serious harm threshold.

In the summer of 2004, Jeremy Stoppelman was sick. He had caught the flu, and was having difficulty locating a suitable physician for treatment. Unsatisfied and increasingly frustrated, Stoppelman began thinking about ways consumers could share recommendations for local services. A few short months later, Yelp was born.[1]

Stoppelman was one of the first to recognise the power of electronic word-of-mouth – or e-WOM, as it has been called[2] – in the search for physicians. In the 17 years since its conception, Yelp has grown to become one of the most commonly used sources of reviews for physicians in Australia, alongside such websites as Google Reviews, RateMDs, Vitals, HealthGrades, RealSelf, and Whitecoat.[3] The success of these websites, which can collectively be referred to as physician-review websites ('**PRWs'**) suggests that online expression of opinion is experiencing a shift. This revolution in user-generated content has been given a name: Web 2.0.[4] Web 2.0 represents a break from static and traditional forms of internet use. In Web 2.0, users are given the opportunity to share their opinions in a way that is both highly visible and highly impactful. By participating in this dynamic and continuous information exchange,[5] users go from being passive receivers of information to the source of information themselves.

Despite its undoubted benefits, Web 2.0 poses new challenges for the tort of defamation. Specifically, the rise of PRW defamation claims in Australia, particularly in the Federal Court, has illuminated the preliminary difficulties that claimants face in their pursuit of a suitable respondent. The exact nature of these hurdles will depend on whether an applicant chooses to pursue the original author of a review or the PRW that hosted it: if the former; the applicant may need to navigate a range of preliminary discovery technicalities; if the latter, the applicant will need to accept the costs and risks of litigating against a foreign entity. Recognising the expense and delay created by such hurdles, legislatures have sought to encourage the early resolution of disputes and prevent trivial claims from reaching the courts. In Australia, this has meant that applicants will now need to overcome an additional set of statutory hurdles before bringing a claim.

The *Model Defamation Amendment Provisions 2020* introduce two new threshold mechanisms by which early dispute resolution may be achieved.[6] The first is that the applicant provide the respondent with a concerns notice that allows the publisher 28 days to make an offer of amends.[7] This requirement, however, is presently being re-evaluated as part of the second stage of reforms, and falls beyond the scope of this article.[8] The other requirement introduced by the *Model Defamation Amendment Provisions* is that the applicant demonstrate that the publication of defamatory matter has caused, or is likely to cause, serious harm to their reputation.[9] Guided by existing UK jurisprudence, this article will present a forward-looking assessment of how this new requirement may operate in the Australian legal landscape with respect to PRW defamation claims. It concludes that the threshold is not unduly restrictive for aggrieved physicians, and that this position is consistent with the aims of defamation law.

I The Development and Interpretation of Serious Harm

The need to consider the relationship between the level of harm caused and the success of a claim is not a novel concept in defamation law. Alongside the recently-repealed statutory defence of triviality, Australian case

1 Laura Hutton, 'AIB Featured Business Leader – Jeremy Stoppelman' *AIB Blog* (Blog Post, 11 April 2017) < https://www.aib.edu.au/blog/business-leaders/featured-business-leader-jeremy-stoppelman/>; Angus Loten, 'Search for Doctor Leads to Yelp', *Wall Street Journal* (online, 14 November 2012) <https://www.wsj.com/articles/SB10001424127887324595904578117512589717352>.

2 Thorsten Henning-Thurau et al, 'Electronic Word-of-Mouth via Consumer-Opinion Platforms: What Motivates Consumers to Articulate Themselves on the Internet?' (2004) 18(1) *Journal of Interactive Marketing* 38. For an overview of existing definitions of eWOM, see Elvira Ismagilova et al, 'Electronic Word-of-Mouth (eWOM)' in Elvira Ismagilova et al (eds) *Electronic Word of Mouth (eWOM) in the Marketing Context: A State of the Art Analysis and Future Directions* (Springer International Publishing, 2017) 17.

3 Heather J Furnas et al, 'Patient Reviews: Yelp, Google, Healthgrades, Vitals, and RealSelf' (2020) 146(6) *Plastic and Reconstructive Surgery* 1419.

4 Tim O'Reilly and John Battelle, 'Opening Welcome' (Speech, State of the Internet Industry Forum, 5 October 2004).

5 Jiyao Xun and Jonathan Reynolds, 'Applying Netnography to Market Research: The Case of the Online Forum', (2010) 18(1) *Journal of Targeting, Measurement and Analysis for Marketing* 17, 21.

6 Explanatory Note, Defamation Amendment Bill 2020 (NSW) 4, 5.

7 Australasian Parliamentary Counsel's Committee, *Consolidated Model Defamation Amendment Provisions 2020* (27 July 2020) ('*Model Defamation Amendment Provisions 2020*') <https://pcc.gov.au/uniform/2020/Consolidated_Model_Defamation_Provisions.pdf>.

8 The current concerns notice and offer to amends process were designed with traditional publishers in mind. The Council of Attorneys General is currently evaluating whether and how these procedures could be amended to apply to internet intermediaries: Council of Attorneys-General, *Review of Model Defamation Provisions – Stage 2* (Discussion Paper, March 2021) ('*MDP Stage 2 Review*') 45, 64–72.

9 *Model Defamation Amendment Provisions 2020* (n 7) s 10A. Additional limitations are imposed on defamation claims made by excluded corporations: at sub-s (2); s

law has flirted with the notion of a minimum threshold of seriousness and principle of proportionality.[10] Moreover, Australian courts benefit from UK jurisprudence concerning the interpretation of its own serious harm requirement.[11] A brief distillation of the themes that have emerged from these decisions allows us to anticipate what Australian courts are likely to consider when assessing serious harm.[12]

Two of the most important common law developments in the area of trivial defamation claims are the cases of *Jameel v Dow Jones & Co Inc* ('*Jameel*')[13] and *Thornton v Telegraph*.[14] While space constraints prevent a detailed consideration of these cases,[15] it is from their 'twin-track approach' that *Defamation Act 2013* (UK) s 1(1) evolved.[16] Both cases represent independent mechanisms by which trivial claims can be eliminated from the courts: following *Jameel*, pointless claims that would be a disproportionate drain on judicial resources may be dismissed as an abuse of process;[17] following *Thornton*, claims that fail to meet a minimum threshold of seriousness will not be considered defamatory.[18] While the serious harm requirement 'builds on' *Thornton* and *Jameel*, it should be emphasised that s 1(1) significantly raises the bar for bringing a claim.[19]

One of the most significant changes effected by s 1(1) *Defamation Act 2013* (UK) relates to its interaction with common law. At common law, defamation has long been actionable *per se*.[20] This raises questions about whether statute now abrogates, by necessary implication, the presumption of damage.[21] Following a period of inconsistency in the law, the UK Supreme Court resolved this issue in *Lachaux v Independent Print Limited* (***Lachaux***).[22] Unanimously rejecting the Court of Appeal's prior finding that serious harm could be established merely on the words' inherent tendency,[23] the Court returned to the interpretation favoured by Warby J at first instance: that claimants must demonstrate, on the balance of probabilities, the *actual or likely* impact of publication.[24] This is to be determined by reference to a combination of the inherent tendency of the words and actual evidence about their impact.[25]

Consequently, *Lachaux* confirms that s 1(1) is to be read as intending a factual investigation of the circumstances surrounding publication.[26] No longer is the court confined, as it was in *Thornton*, to the objective seriousness of the words: a wide range of contextual matters, ranging from the credibility of the publisher[27] to the breadth of publication,[28] may now be considered as part of the court's assessment of serious harm.[29] In the likely event that Australian courts will take guidance from UK jurisprudence on this point,[30] we can expect to see courts engaging in thorough circumstantial investigation as part of their assessment.

II Proving serious harm in PRW defamation cases

Given the forensic demands created by the new threshold, it has been suggested that it may be difficult for single private individuals to establish that they have suffered serious harm to reputation.[31] However, PRW defamation cases have unique features that may increase a court's willingness to find the threshold satisfied, at least in the case of competent and honest physicians.

A Nature and meaning of reviews

Web 2.0 has transformed not only the way that people communicate, but the language they use to do so. As was put by one judge, online communication no longer has 'the formality and the careful consideration that was once

9(1). However, considering the trend that doctors sue individually rather than on behalf of their clinical practice, this section will not be addressed.

10 See generally Kim Gould, 'Locating a Threshold of Seriousness in the Australian Tests of Defamation' (2017) 39(3) *Sydney Law Review* 333; David Rolph, 'Triviality, Proportionality and the Minimum Threshold of Seriousness in Defamation Law' (2019) 23(3) *Media and Arts Law Review* 280.

11 *Defamation Act 2013* (UK) s 1(1).

12 For a detailed consideration of the historical development of the serious harm requirement in the UK, see Phoebe J Galbally, 'A "Serious" Response To Trivial Defamation Claims: An Examination of s 1(1) of the *Defamation Act 2013* (UK) From An Australian Perspective' (2015) 20(3) *Media and Arts Law* Review 213; Alastair Mullis and Andrew Scott, 'Tilting at Windmills: The Defamation Act 2013' (2014) 77(1) *Modern Law Review* 87.

13 [2005] QB 946 ('*Jameel*').

14 [2010] EWHC 1414 (QB) ('*Thornton*').

15 See n 12.

16 *Lachaux v Independent Print Ltd* [2016] QB 402, [50] (Warby J).

17 *Jameel* (n 13).

18 *Thornton* (n 14).

19 Explanatory Notes, Defamation Act 2013 (UK) [11].

20 *Uren v John Fairfax & Sons Ltd* (1966) 117 CLR 118 at 150 (Windeyer J); *Bristow v Adams* [2012] NSWCA 166.

21 David Rolph, 'A Critique of the Defamation Act 2013: Lessons for and from Australian Defamation Law Reform' 2016 21(4) *Communications Law* 116, 119.

22 [2019] UKSC 27 ('*Lachaux*').

23 Ibid [14]–[17] (Lord Sumption for the Court). See also *Thornton* (n 14) [95].

24 *Lachaux* (n 22) [20] (Lord Sumption for the Court); *Lachaux v Independent Print Ltd* [2016] QB 402, [45]–[47] (Warby J).

25 *Lachaux* (n 22) [12], [14] (Lord Sumption for the Court). However, proof will not be required in circumstances where the words are so obviously serious that harm can be inferred: *Cooke & Anor v MGN Ltd & Anor* [2014] EWHC 2831 (QB) [43] (Bean J).

26 See also *Cooke & Anor v MGN Ltd* (n 279); *Theedom v Nourish Training* [2015] EWHC 3769 (QB) [28] (Moloney J).

27 See, eg, *Monroe v Hopkins* [2017] EWHC 433 (QB), [71] (Warby J).

28 See, eg, *Ames v Spamhaus Project Ltd* [2015] 1 WLR 3409, 3428–3429 [70] (Warby J); *Lachaux v Independent Print Ltd* [2016] QB 402, [139] (Warby J).

29 For an empirical analysis of the themes discussed in UK serious harm cases, see Charlie Sewell, 'More Serious Harm than Good? An Empirical Observation and Analysis of the Effects of the Serious Harm Requirement in Section 1(1) of the Defamation Act 2013' (2020) 12(1) *Journal of Media Law* 47.

30 As Gould notes, English decisions may not be binding, but may remain persuasive: Kim Gould, 'Locating a Threshold of Seriousness in the Australian Tests of Defamation' (n 10) 335.

31 David Rolph quoted in Josh Taylor, 'Negative Criticism: Can the Surge in Google Review Defamation Cases be Stopped?', *The Guardian* (online, 25 July 2021) <https://www.theguardian.com/law/2021/jul/25/negative-criticism-can-the-surge-in-google-review-defamation-cases-be-stopped>.

thought to mark the difference between the written and the spoken word'.[32] Instead, it has gained notoriety for being 'uninhibited, casual and ill-thought out'.[33] These characteristics increase the potential for trivial defamatory content that falls short of the serious harm threshold.

This risk presents itself clearly in the case of PRWs. Empirical research has shown that online physician reviews have an alarming tendency to focus on clinical practice issues such as wait time, interactions with staff, billing, the quality of the practice environment, and even parking availability.[34] But even where such reviews disproportionally affect a physician's aggregate score, they are likely to be subsumed under the general umbrella of 'matter not to be taken seriously'.[35] Physician applicants appear to understand this. Indeed the PRW defamation cases that have come before the courts in recent years have not been concerned with the trivial remarks of a few disgruntled patients, but reviews of a more malicious variety. The adverse imputations raised by these reviews range from the critical to the downright ludicrous: otherwise capable and reputable doctors have been attacked for their incompetent,[36] unprofessional[37] and negligent[38] service; labelled 'butchers'[39] who perform 'botched' or 'bad' surgery;[40] accused of engaging in 'unethical',[41] 'inhumane'[42] or 'illegal'[43] behaviour; cast as 'fraudsters',[44] 'stealers',[45] 'cheaters',[46] 'bullies'[47] and 'compulsive liars',[48] and, most extreme of all, accused of mutilation[49] or named 'the devil himself'.[50] One can appreciate how even one of these imputations could cause serious harm to a doctor's reputation, let alone reviews which carry multiple imputations.[51]

For this reason, even PRW reviews using amaterurish or hyperbolic language have been found to be highly serious. In *Dean v Puleio*, Clayton J observed that the 'rambling and at times incoherent' content of the reviews that had been left about a periodontist made it unlikely that many people would take them seriously.[52] However, her Honour went on to acknowledge that to some readers – particularly those who have had unpleasant experiences with medical professionals – the 'unreasonableness' of such reviews would not affect the extent to which they are given credence.[53] Such readers would, upon reading such allegations contained within, prefer to 'steer clear' of any doctor with such a review.[54] The decision demonstrates that while the linguistic style of a review is a relevant consideration, it will not always defeat a review's believability.

---

32 *Prefumo v Bradley* [2011] WASC 251, [43] (Corboy J), cited in *Rana v Google Australia Pty Ltd* [2013] FCA 60, [78] (Mansfield J).

33 *Smith v ADVFN Plc* [2008] EWHC 1797 (QB), [13]–[14] (Eady J).

34 See, eg, Chester J Donnally, 'How Social Media, Training, and Demographics Influence Online Reviews Across Three Leading Review Websites for Spine Surgeons' (2018) 18(11) *Spine Journal* 2081; Jesse E Bible et al, 'Are Low Patient Satisfaction Scores Always Due to the Provider? Determinants of Patient Satisfaction Scores During Spine Clinic Visits' (2017) 43(1) *Spine Surgery* 58, 61; Fabia Rothenfluh and Peter J Schulz, 'Content, Quality, and Assessment Tools of Physician-Rating Websites in 12 Countries: Quantitative Analysis' (2018) 20(6) *Journal of Medical Internet Research* e212: 1–14, 7; Martin Emmert et al, 'What Do Patients Say About Their Physicians? An Analysis of 3000 Narrative Comments Posted on a German Physician Rating Website' (2014) 118(1) *Health Policy* 66; Andrea Lopez et al, 'What Patients Say About Their Doctors Online: a Qualitative Content Analysis' (2012) 27(6) *Journal of General Internal Medicine* 685; Guodong Gordon Gao et al, 'A Changing Landscape of Physician Quality Reporting: Analysis of Patients' Online Ratings of Their Physicians Over a 5-Year Period' (2012) 14(1) *Journal of Medical Internet Research* 38.

35 See Kim Gould, 'The Statutory Triviality Defence and the Challenge of Discouraging Trivial Defamation Claims on Facebook' 2014 19(2) *Media and Arts Law Review* 113, 121, citing *Clift v Clarke* [2011] EWHC 1164 (QB), [32] (Sharp J); *Sheffield Wednesday Football Club Ltd v Hargreaves* [2007] EWHC 2375 (QB), [17] (Parkes DJ); *Smith v ADVFN Plc* [2008] EWHC 1797 (QB), [17] (Eady J).

36 *Nettle v Cruse* [2021] FCA 935, [34] (Wigney J); *Tavakoli v Imisides (No 4)* [2019] NSWSC 717, [3] (Rothman J); *Kabbabe v Google LLC* [2020] FCA 126, [15] (Murphy J); *Yuanjun Holdings Pty Ltd and Ors v Min Luo* (Civil) [2018] VMC 7, [53] (Magistrate Ginnane) ('*Yuanjun Holdings v Min Luo*'); *Callan v Chawk* [2021] FCA 1182, [21] (Halley J); *KT v Google LLC* [2019] NSWSC 1015 (Fagan J).

37 *Dean v Puleio* [2021] VCCA 848, [10] (Clayton J), *Yuanjun Holdings v Min Luo* (n 36) [12]–[13] (Magistrate Ginnane).

38 *Yuanjun Holdings v Min Luo* (n 36) [12]–[13] (Magistrate Ginnane).

39 See Jaime McKinnel, 'Doctor Sues Google Over Negative Reviews, But Tech Giant Claims It Is 'Subordinate Distributor', *ABC News* (online, 17 September 2019) <https://www.abc.net.au/news/2019-09-16/google-defamation-case-sydney-doctor-sues/11516182> (discussing the statement of claim in *KT v Google* (n 36)); Leo Shanahan, 'Doctor Sues Over Google Reviews', *The Australian* (online, 3 November 2019) <https://www.theaustralian.com.au/business/media/doctor-sues-over-google-reviews/news-story/737ead4ffb503378b8485f5756bf21e0> (discussing the statement of claim in *Kalus v Google LLC* (Federal Court of Australia, NSD1724/2019, commenced 17 October 2019)). See also *Al Muderis* v Duncan (No 3) [2017] NSWSC 726, [5] (Rothman J) ('*Al Muderis v Duncan*') (concerning defamatory statements made on a website rather than in a review).

40 *Callan v Chawk* (n 36) [21] (Halley J), *Nettle v Cruse* (n 36) [32].

41 *Dean v Puleio* (n 37) [18] (Clayton J), *Nettle v Cruse* (n 36) [20], [26], [38] (Wigney J).

42 *Nettle v Cruse* (n 36) [32] (Wigney J).

43 Ibid [26], [40] (Wigney J); see n 39.

44 *Nettle v Cruse* (n 36) [38], [40]; see n 39.

45 See n 39.

46 *Nettle v Cruse* (n 36) [38] (Wigney J).

47 *Dean v Puleio* (n 37) [10] (Clayton J). See *Al Muderis* v Duncan (n 293) [6] (Rothman J).

48 *Nettle v Cruse* (n 36) [26], [32] (Wigney J).

49 *Al Muderis* v Duncan (n 39) [11] (Rothman J).

50 *Nettle v Cruse* (n 36) [32] (Wigney J).

51 Indeed the trend that emerges from the case law is that when reviewers write with malicious intent, they tend to adopt a 'no holds barred' approach, with some reviews carrying over nine imputations from the same matter: see *Dean v Puleio* (n 37) [18] (Clayton J); *Nettle v Cruse* (n 36) [34] (Wigney J).

52 *Dean v Puleio* (n 37) [26] (Clayton J).

53 Ibid.

54 Ibid.

B Actual impact of reviews

As established earlier, that the words of a review carry an 'inherent tendency' to cause harm will be insufficient, in and of itself, to meet the serious harm threshold.[55] The applicant will also need to establish on the balance of probabilities that those words have caused, or will cause, reputational harm.[56] Corinna Coors has argued that this new threshold will in principle 'allow negative reviews to be swamped by positive reviews if they are sufficient to eradicate or at least minimise any unfavourable impression created by the original review'.[57] For reasons that shall become apparent, positive reviews are unlikely to have this effect.

Research suggests that negative reviews, however few, have a greater impact than many positive reviews.[58] The impact of this so-called negativity bias in the context of PRWs is apparent, with studies showing that of patients who have used reviews to choose a physician, between 37%[59] and 52%[60] report that negative reviews have led them to seek care elsewhere. This is corroborated by the facts of recent cases. In the case of *Nettle v Cruse*, for example, evidence indicated that prior to the impugned publications the online reviews of Dr Nettle were overwhelmingly positive: he had a 5-star Google review rating.[61] Notwithstanding the 'exceptional' online reputation the Bondi surgeon had built,[62] one of Dr Nettle's patients testified that upon reading the reviews, she 'started to have doubts and think twice about continuing to see Dr Nettle', and that 'she felt she could no longer trust [him]'.[63] As the Court itself recognised, it is reasonable to infer that other patients – existing or prospective – would have had a similar reaction to such reviews.[64] Dr Nettle himself also testified that that his workload declined significantly following the publication of the defamatory reviews.[65]

Applicants in comparable cases have raised similar examples of actual harm. In *Dean v Puleio*, evidence was given of the distinct downturn in average weekly page views of the applicant's website and in new-patient referrals.[66] Data review in *Tavakoli v Imsidies* revealed that the rate of visitors to the applicant's website had dropped by nearly a quarter in less than one week after the review had been posted. In *Yuanjun Holdings v Min Luo,* the applicant observed that 'all of a sudden the phone stopped ringing'.[67] These are highly significant pieces of evidence. Recent systematic review indicates that more than half of physicians listed on PRWs have no ratings or reviews at all, and that even where physicians *were* rated, most had only one to three reviews.[68] This skewing effect therefore not only limits the credibility of PRWs, but can have a disproportionate impact: given the low prevalence of ratings, a single unfavorable rating can decrease a physician's average score and 'make an otherwise high-performing physician appear mediocre'.[69] Considering that so many physicians now rely on the internet to attract patients,[70] the harm caused will often be significant and immediate.

In order to understand why a single disparaging review can have such a dramatic effect, regard must be had to the special quality of a physician's reputation. In *Crampton v Nugawela*, it was observed that 'in some cases, a person's reputation is, in a relevant sense, his whole life'.[71] The reputation of doctors can be said to be of this character: as was put plainly by the Court in both *Tavakoli and Imisides*[72] and *Nettle v Cruse*,[73] their 'whole life depends upon [their] honesty and [their] competence'. Reviews that cast aspersions over a doctor's integrity or judgment therefore go to the very heart of their life's work.[74]

---

55 *Lachaux* (n 22) [14], [16] (Lord Sumption for the Court).

56 Gould, 'Locating a Threshold of Seriousness in the Australian Tests of Defamation' (n 10) 344, citing *Lachaux* [2016] QB 402, 419–20, 424.

57 Corinna Coors, 'Opinion or defamation? Limits of free speech in online customer reviews in the digital era' (2015) 20(3) *Communications Law* 72, 73.

58 Krishn Khanna and Mohammad Diab, 'Physician Ratings: Determinants, Accuracy, and Impact' (2021) 103(7) *Journal of Bone and Joint Surgery* e27, e27(4); Siyue Li and Austin Hubner, 'The Impact of Web-Based Ratings on Patient Choice of a Primary Care Physician Versus a Specialist: Randomized Controlled Experiment' (2019) 21(6) *Journal of Medical Internet Research* e11188: 1–12, 9; Nima Kordzadeh, 'Investigating Bias in the Online Physician Reviews Published on Healthcare Organizations' Websites' [2019] (118) *Decision Support Systems* 70, 79. For the effect of negativity bias in the context of review sites generally, see Dezhi Yin, Sabyasachi Mitra and Han Zhang, 'When Do Consumers Value Positive vs. Negative Reviews? An Empirical Investigation of Confirmation Bias in Online Word of Mouth' (2016) 27(1) *Information Systems Research* 131.

59 David A Hanauer, 'Public Awareness, Perception, and Use of Online Physician Rating Sites' (2014) 311(7) *Journal of the American Medical Association* 734.

60 Martin Emmert et al, 'Physician Choice-Making and Characteristics Associated with Using Physician-Rating websites: Cross-Sectional Study' (2013) 15(8) *Journal of Medical Internet Research* e187.

61 *Nettle v Cruse* (n 36) [49] (Wigney J).

62 Ibid.

63 Ibid [50].

64 Ibid. See also *Dean v Puleio* (n 37), in which another physician gave evidence that reviews 'would most certainly have had an impact on the referral base of dentists and any potential clients': at [22] (Clayton J).

65 *Nettle v Cruse* (n 36) [53] (Wigney J).

66 *Dean v Puleio* (n 37) [27] (Clayton J).

67 *Yuanjun Holdings v Min Luo* (n 36) [26], [86]–[87] (Magistrate Ginnane).

68 Pavankumar Mulgund et al, 'Data Quality Issues With Physician-Rating Websites: Systematic Review' (2020) 22(9) *Journal of Medical Internet Research* e15916: 1–12, 6, citing Haijing Hao et al, 'A Tale of Two Countries: International Comparison of Online Doctor Reviews between China and the United States' [2017] (1) *International Journal of Medical Informatics* 37.

69 Chandy Ellimoottil, 'Online Physician Reviews: The Good, the Bad, and the Ugly' (2013) 98(9) *Bulletin of the American College of Surgeons* 34, 36; Samir K Trehan and Aaron Daluiski, 'Online Patient Ratings: Why They Matter and What They Mean' 2016 41(2) *Journal of Hand Surgery* 316.

70 See judicial comments made in *Kabbabe* (n 36) [1] (Murphy J) and *Dean v Puleio* (n 37) [22] (Clayton J).

71 [1996] NSWSC 651 (Mahoney ACJ).

72 *Tavakoli v Imisides (No 4)* (n 36) (62);

73 *Nettle v Cruse* (n 36) [54] (Wigney J).

74 Ibid [54]; *Tavakoli v Imisides (No 4)* (n 36) [77] (Rothman J). See also Sean D Lee, '"I Hate My Doctor": Reputation, Defamation, and Physician-Review Websites' (2013) 23(2) *Health Matrix* 573.

Australian PRW defamation cases that have progressed to full trial show sensitivity to this idea. In such cases, Courts have acknowledged that prior to the disparaging reviews, the physicians in question had been held in high regard.[75] Nowhere in these cases has it been suggested that having an illustrious reputation somehow negates the damage caused by negative reviews. To the contrary: courts have been very sympathetic to the plight of doctors who have worked for many years to establish a good standing in their professional circles and among patients.[76] Courts may therefore be quite prepared to find that a defamatory review results in demonstrable harm even where a physician typically enjoys a robust reputation.[77]

However Australian courts go on to interpret the new serious harm requirement, the requirement that serious harm be dealt with as a threshold issue is a serious development in the law.[78] Certainly, it increases delays at the beginning of the trial and exposes the applicant to costs that may well be 'wholly disproportionate to the value of obtaining an answer'.[79] But ultimately, this 'frontloading'[80] is not likely to be an unduly cumbersome hurdle for claimants in PRW defamation claims. The law remains fundamentally plaintiff-friendly. Moreover, this position can be justified.

Competent physicians deserve protection from untrue slurs. With an increasing number of cases involving online reviews and physicians coming before the Federal Court, we are already seeing the legal consequences of the new and complex dynamic that PRWs represent. Less visible but even more insidious are the psychological consequences of unfair PRW usage: physicians are practicing more defensively[81] and reporting reporting higher job stress,[82] behaviours which could jeopardise patient safety, increase physician turnover, and create other challenges to the delivery of high-quality care.[83]

Given these unfair impacts, it can hardly be surprising that physicians are fighting back. Just as patients are moving away from paternalistic models of care, so too are physicians moving away from the historical reluctance to take legal action against their patients.[84] While this may appear to some to disturb foundational principles of beneficence and nonmaleficence,[85] the reality is that physicians cannot opt out of the internet. If patients – or competitors posing as patients – cannot be trusted to leave fair and honest reviews, defamation law will provide an absolutely essential mechanism by which physicians can safeguard their professional reputations. Without its protections, physicians may be left without a remedy in circumstances where a remedy is vital.

---

75 See, eg, *Tavakoli v Imisides (No 4)* (n 36) [75] (Rothman J); *Nettle v Cruse* (n 36) [48] (Wigney J); *Dean v Puleio* (n 37) [23]–[26] (Clayton J).

76 *Dean v Puleio* (n 37) [21–25] (Clayton J); *Nettle v Cruse* (n 36) [47–48] (Wigney J); *Tavakoli v Imisides (No 4)* (n 36) [75] (Rothman J). See also *Al Muderis v Duncan* (n 39) [44]–[64] (Rothman J).

77 Cf Coors (n 57).

78 Rolph, 'Triviality, Proportionality and the Minimum Threshold of Seriousness in Defamation Law' (n 10) 301.

79 Evidence to Joint Committee on the Draft Defamation Bill, House of Lords Paper No 203, House of Commons Paper No 930–III (2011) vol III, 175 [6], 176 [10]–[11] (Mark Warby QC), quoted in James O'Hara, 'Defamation: Serious Harm and Contextual Truth' (2021) 95(5) *Australian Law Journal* 348, 366.

80 Galbally (n 12) 223, citing Ministry of Justice, 'Draft Defamation Bill: Summary of Responses to Consultation' (Consultation Paper CP3/11, 24 November 2011).

81 Incorrectly incentivised by the promise of positive reviews or even better remuneration, PRWs may encourage what has described as 'defensive medicine': the practice of ordering needless tests or treatments in order to maximise patient satisfaction: James E Sabin, 'Physician-Rating Websites' (2013) 15(11) *Virtual Mentor* 932, 935, cited in Trehan, Samir K and Aaron Daluiski, 'Online Patient Ratings: Why They Matter and What They Mean' 2016 41(2) *Journal of Hand Surgery* 316, 318.

82 Alison M Holliday et al, 'Physician and Patient Views on Public Physician Rating Websites: A Cross-Sectional Study' (2017) 32(6) *Journal of General Internal Medicine* 626, 630/

83 Ibid citing Colin P West, 'Physician Well-Being: Expanding the Triple Aim' (2016) 31(5) *Journal of General Internal Medicine* 458.

84 Ian Freckleton and Tina Popa, 'Doctors, Defamation and Damages' (2019) 27(1) *Journal of Law and Medicine* 20.

85 Ian Freckelton, 'Vindication of Professional Reputation Arising from Defamatory Online Publications' (2020) 11(1) *Beijing Law Review* 382, 385.

About CAMLA

The Communications and Media Law Association Incorporated (CAMLA) brings together a wide range of people interested in law and policy relating to communications and the media. CAMLA includes lawyers, journalists, broadcasters, members of the telecommunications industry, politicians, publishers, academics and public servants.

Issues of interest to CAMLA members include:

- Defamation
- Contempt
- Broadcasting
- Privacy
- Copyright
- Censorship
- Advertising
- Film Law
- Information Technology
- Telecommunications
- Freedom of Information
- The Internet & Online Services

In order to debate and discuss these issues CAMLA organises a range of seminars featuring speakers prominent in communications and media law policy.

Speakers have included Ministers, Attorneys-General, members and staff of communications regulatory authorities, senior public servants, executives in the communications industry, lawyers specialising in media and communications law, and overseas experts.

CAMLA provides a useful way to establish informal contacts with other people working in the business of communications and media. It is strongly independent, and includes people with diverse political and professional connections. To join CAMLA, or to subscribe to the Communications Law Bulletin, complete the form below and forward it to CAMLA.

Disclaimer

The Communications Law Bulletin is the journal of the Communications and Media Law Association which is an independent organisation which acts as a forum for debate and discussion and welcomes the widest range of views. The views expressed in the Communications Law Bulletin and at CAMLA functions are personal views of the respective authors or speakers. They are not intended to be relied upon as, or to take the place of, legal advice.

For Further Information:

Visit the CAMLA website at: **www.camla.org.au** for information about CAMLA, CAMLA seminars and events, competitions and the Communications Law Bulletin.

To: The Secretary, contact@camla.org.au or
CAMLA, PO Box 345, HELENSBURGH NSW 2508
Phone: 02 42 948 059

Name: .....

Address: .....

Telephone: ..... **Fax:** .....

Email: .....

Principal areas of interest: .....

I hereby apply for the category of membership ticked below, which includes a Communications Law Bulletin subscription, and enclose a cheque in favour of CAMLA for the annual fee indicated:

☐ **Ordinary membership $140** (includes GST)

☐ **Student membership $45** (includes GST)
(include undergraduate full time student card copy)

☐ **Corporate membership $595** (includes GST)
(include a list of names of individuals - maximum 5)

☐ **Subscription without membership $150** (includes GST) (Library subscribers may obtain extra copies for $10.00 each + GST and handling)