CAMLA COMMUNICATIONS LAW
BULLETIN
Communications & Media Law Association Incorporated
Volume 39, No 2. June 2020

COVID Communications:

How Fake News Fanned Coronavirus Hysteria

And should intermediaries be held responsible for online falsehoods?

Rachel Baker, Lawyer, Clayton Utz, discusses fake news and disinformation in the coronavirus context, and looks at the legal responsibilities of internet intermediaries.

As the novel coronavirus spread around the world in early 2020, online falsehoods about the pandemic were also going viral. Some of these falsehoods (such as whether smoking cannabis could prevent the virus) were little more than light entertainment, but others increased the hysteria in already tense communities, prompting individuals to engage in dangerous and even criminal behaviour. In Australia, there is legislation creating obligations in relation to electoral advertising and there is of course the risk of a suit for defamation or other civil wrongs. However, there is no prohibition on producing or distributing material whose only harm is that it is untrue. Regulators around the world are concerned at the growing influence of online falsehoods, sometimes referred to as "fake news" and some governments are considering whether internet intermediaries can be held liable for their role as platforms on which this material is published. Part of the challenge involves defining "fake news"; while it is a term used in various contexts to convey a range of meanings, it is popularly understood as meaning deliberately false information spread via traditional or social media that intends to manipulate the public, and this article uses that meaning. Regulators are concerned that, unlike other types of falsehood, fake news has heightened power to cause social harm and justifies special legal treatment. Such sentiment raises questions not only about the practicality of enforcement but also whether banning fake news would come at the price of placing an unbearably high burden on free speech.

5G network and coronavirus

One prominent piece of fake news during the coronavirus pandemic has been that the 5G mobile network causes the virus. More specifically, this is a cluster of theories: that coronavirus is not contagious but is an illness caused by exposure to radiation from the 5G network, that the 5G network weakens your immune system and makes you more vulnerable to the effects of coronavirus, and that lockdowns are being used as cover to install 5G networks. The link between 5G and the virus appears to have first been made by a Belgian doctor in January. Newspaper *Het Laatste Nieuws* published an interview with general practitioner Dr Kris Van Kerckhoven who said that 5G was dangerous and might be linked to coronavirus.[1]

1 'How the 5G coronavirus conspiracy theory tore through the internet', Wired, 6 April 2020, accessed online at https://www.wired.co.uk/article/5g-coronavirus-conspiracy-theory.

Contents

CAMLA

Editors
Ashleigh Fehrenbach and Eli Fisher

Editorial Assistants
Isabella Street and Claire Roberts

Design | Printing | Distribution
MKR Productions

Editors' Note

2020 is certainly shaping up to be a year for the record books. This rather unique year in Australia is also seeing exciting developments in the privacy and defamation spaces. The June edition of the CLB features **Katherine Sainty** and **Belyndy Rowe's** (Sainty Law) take on the Privacy Commissioner's claim against Facebook in relation to Cambridge Analytica and the platform's alleged "serious and/or repeated interferences" with privacy in contravention of Australian privacy law**. Rachel Baker** (Clayton Utz) takes us through the recent bouts of fake news and disinformation in the coronavirus context, and looks at the legal responsibilities of internet intermediaries. **Will Sharpe** (HWL Ebsworth) discusses the recent *Smethurst v Commissioner of Police* decision where the High Court weighed up confidentiality, privacy and public interest considerations in refusing an order for destruction of material seized under warrant. This case makes some important observations on what practical recourse is available to a private citizen when a Commonwealth official exceeds its powers.

Defamation suits and injurious falsehood claims are also having their time in the sun. **Adaena Sinclair-Blakemore** (Baker McKenzie) analyses the recent *Omega Plumbing v Harbour Radio* judgment, which looks at establishing malice in injurious falsehood proceedings and **Nicole Phillips** (Arnold Bloch Leibler) discusses the rise of Google review defamation suits in Australia. Big tech companies are not the only ones experiencing some pivots in this area. **Marlia Saunders** (News Corp Australia) takes us through the lessons from the recent Hubba Bubba case and why not to sue for defamation (or, at least, to settle early). Daniel Johns of Silverchair fame may have utilised these learnings in his recent stoush with the Sunday Telegraph case against him, which has since been settled with an apology.

Our CLB editor **Eli Fisher** (Baker McKenzie), profiles **Melissa Sequeira** Legal Manager and Company Secretary at ViacomCBS Networks (Pay) ANZ, to chat about her career and her reflections on this unique time. And we provide details within for the **CAMLA Young Lawyers Prepub 101 webinar on 25 June 2020** and the **CAMLA Essay Competition**.

We hope you enjoy the read as much as we enjoyed putting it together.

Ashleigh and Eli

News of a potential link became popular on Dutch speaking social media, then spread to the English speaking internet, but was mainly confined to relatively obscure talk show hosts and vloggers. What happened then – according to theories from some technology commentators – is that the engagement algorithms used by social media platforms detected that this content was becoming a viral trend, which propelled it to greater prominence.[2] Before long, Hollywood celebrities were passing on these rumours as fact. At one point, there were more than 50,000 posts about 5G and coronavirus within a 24 hour period.[3] An online disinformation specialist at Khalifa University in Qatar, Marc Owen Jones, claimed the rumour had the hallmarks of a state-backed campaign.[4] There is no confirmation yet of a state actor starting the 5G coronavirus rumour but The *New York Times* last year reported that Russian television network RT America has spread other falsehoods designed to undermine 5G technology (suggesting it causes brain cancer, infertility, autism and Alzheimer's disease), in an apparent effort to slow its rollout in the West (so that Russia can catch up and gain a competitive advantage).[5] The rumours struck a chord with the general public: in mid-April, more than 50 mobile towers were vandalised over one weekend alone in the United Kingdom;[6] there were similar incidents in other countries,[7] apparently in protest at the supposed health risks posed by the technology. Australian telecommunications company Telstra issued a statement seeking to dispel the myth.[8]

Platforms acted to remove the content. YouTube announced that videos linking 5G and coronavirus breached its policies against promoting unsubstantiated coronavirus prevention methods and in early April began actively removing all such content.[9] Soon after, Facebook followed suit.[10] Many platforms are prominently displaying authoritative health information from sources such as the World Health Organisation and Australian Government in an effort to drive traffic towards more reliable sources.

International regulation of fake news

Fake news of course pre-dates the coronavirus pandemic and many authorities have in recent years begun taking steps to reduce the harm it can cause. In some jurisdictions, this involves holding intermediaries responsible for false content that is not otherwise unlawful.

In May 2019 Singapore passed legislation criminalising the dissemination of false information online. The *Protection from Online Falsehoods and Manipulation Act 2019* makes it illegal to spread "false statements of fact" that compromise security or public safety. It gives any government Minister the power to direct an internet intermediary to disable access to false material and publish a correction notice. The legislation has been criticised by

2 Ibid.
3 '5G Virus Conspiracy Theory Fueled by Coordinated Effort', Bloomberg, 9 April 2020, accessed online at https://www.bloomberg.com/news/articles/2020-04-09/covid-19-link-to-5g-technology-fueled-by-coordinated-effort.
4 Ibid.
5 'Your 5G Phone Won't Hurt You. But Russia Wants You to Think Otherwise', *New York Times*, 12 May 2019, https://www.nytimes.com/2019/05/12/science/5g-phone-safety-health-russia.html
6 'Over 50 Cell Towers Vandalized in UK Due to 5G Coronavirus Conspiracy Theories', *PC Mag*, 15 April 2020, accessed online at https://au.pcmag.com/digital-life/66385/over-50-cell-towers-vandalized-in-uk-due-to-5g-coronavirus-conspiracy-theories.
7 'Coronavirus: Far North cell tower vandalism linked to Covid-19 conspiracy theory', *stuff.co.nz*, 13 April 2020, accessed online at https://www.stuff.co.nz/national/crime/120985809/coronavirus-far-north-cell-tower-vandalism-linked-to-covid19-conspiracy-theory
8 Telstra website: https://exchange.telstra.com.au/5g-health-concerns-and-covid-19-the-facts/
9 'YouTube will delete videos that falsely link 5G to the novel coronavirus after reports of people setting phone masts on fire', *Business Insider Australia*, 6 April 2020, accessed online at https://www.businessinsider.com.au/youtube-delete-5g-coronavirus-conspiracy-2020-4?r=US&IR=T.
10 'Facebook removes David Icke coronavirus-5G conspiracy video', ITV *Report*, 19 April 2020, accessed online at https://www.itv.com/news/2020-04-09/facebook-removes-david-icke-coronavirus-5g-conspiracy-video/.

human rights groups and journalists for restricting free speech and giving government ministers broad, discretionary powers to censor criticism.[11]

In the United States, after intelligence agencies confirmed interference by Russia in the 2016 Presidential election[12], several states passed laws requiring schools to increase media literacy programs for students.[13] The *Honest Ads Act*, requiring greater transparency in political advertising on internet platforms, was introduced into the US Senate in 2017, but has not yet been made law.[14]

The United Kingdom has held an inquiry into Disinformation and Fake News which recommended that clear legal liabilities be established for technology companies to act against harmful content on their sites, coupled with independent regulation and a compulsory Code of Ethics, setting out what constitutes harmful content.[15] The UK Government has issued an Online Harms White Paper which sets out reforms to deal with a range of problematic content, including a statutory duty of care by technology companies to their users.[16] However, following a period of public consultation, the UK Government confirmed that the regulator will not require the removal of material that is legal but potentially harmful and will instead "require companies, where relevant, to explicitly state what content and behaviour they deem to be acceptable on their sites and enforce this consistently and transparently."[17]

Sweden is taking action on the consumer side, establishing a government agency tasked with developing the nation's "psychological defence". The agency will seek to ensure that factual information can be communicated quickly and effectively. It will also seek to identify, analyse and confront influencing operations.[18]

Regulation in Australia

In Australia, the Federal Government's response to the Australian Competition and Consumer Commission's Digital Platforms Inquiry final report indicated that it will ask major digital platforms to develop a voluntary code (or codes) of conduct for disinformation and news quality.[19] The codes will outline what steps the platforms will take to tackle disinformation on their services and help consumers assess the quality of news and information they access online. The government says the codes will be based on international examples, such as the European Union Code of Practice on Disinformation (EU code), which was agreed to by major digital platforms and advertisers in 2018.[20]

The EU code requires platforms to "disrupt advertising revenues" of accounts and sites known for spreading disinformation, provide users with more information about the origins of political and issue-based advertising, give greater prominence to authoritative content, and make it easier to report the occurrence of fake news.[21] Efforts to disrupt and provide greater transparency around paid content will no doubt assist the battle against fake news but will not address the phenomenon of disinformation gaining popularity in the community and being voluntarily spread through individual accounts without payment, as occurred with the 5G coronavirus fake news. Indeed, the prevalence of 5G disinformation makes clear that the EU code has not eradicated fake news in Europe.

If Australia were to seek further regulation of fake news, some of the challenges facing legislators will include the difficulty in determining what is false, and even greater difficulty in determining what is deliberately false and manipulative. Enforcement by way of suspending offending accounts can also be fraught when disinformation starts as on offline rumour which is then spread (without malicious intent) by individuals who believe it to be true.

Whichever method regulators seek to employ, it is important they remain cognisant of the fact that not all untruths are harmful. Even if it were practically possible to rid the internet of all lies (or more specifically all statements lacking factual basis), there is doubt as to whether that would be a desirable outcome. The expression of unsupported ideas that challenge orthodoxy can trigger debate, research and learning, all of which are vital in democratic societies. To stamp out the expression of views that cannot be proven true would be dangerous and undesirable. Achieving the best outcome, in terms of protecting society from false news, while allowing the community to enjoy the benefits of open communication in a thriving digital economy, will likely involve providing internet users with greater transparency about the origins of sponsored posts (as required under the EU code) coupled with education to encourage consumers to question the accuracy and motivations of material read online.

11 'Singapore's fake news law: protecting the truth, or restricting free debate?', *SCMP,* 21 December 2019, accessed online at https://www.scmp.com/week-asia/politics/article/3043034/singapores-fake-news-law-protecting-truth-or-restricting-free.

12 2016 Presidential Campaign Hacking Fast Facts, *CNN*, 31 October 2019, accessed online at https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html.

13 'California now has a law to bolster media literacy in schools', *The Press Democrat*, 18 September 2018, accessed online at https://www.pressdemocrat.com/news/8754461-181/california-now-has-a-law.

14 'Senators announce new bill that would regulate online political ads', The Verge, 19 October 2017, accessed online at https://www.theverge.com/2017/10/19/16502946/facebook-twitter-russia-honest-ads-act; https://en.wikipedia.org/wiki/Honest_Ads_Act

15 , 'Disinformation and 'fake news': Final Report', Culture, Media and Sport Committee, chapter 2 [37], accessed online at https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179105.htm#_idTextAnchor006.

16 'Online Harms White Paper', UK Government (Department for Digital, Culture, Media and Sport and Home Office), updated 20 February 2020, page 41, accessed online at https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper.

17 Online Harms White Paper Initial Consultation Response, UK Government (Department for Digital, Culture, Media and Sport and Home Office), 12 February 2020, accessed online at https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response.

18 'Sweden to create new authority tasked with countering disinformation', *The Local*, 15 January 2018, accessed online at https://www.thelocal.se/20180115/sweden-to-create-new-authority-tasked-with-countering-disinformation.

19 'Government Response and Implementation Roadmap for the Digital Platforms Inquiry', 12 December 2019, Australian Government (Treasury), page 7, accessed online at https://treasury.gov.au/publication/p2019-41708.

20 European Commission website: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

21 European Commission Website: https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation

Death by Rating - The Rise of Google Review Defamation Suits in Australia

Nicole Phillips, lawyer at Arnold Bloch Leibler, discusses the new line of cases in the Federal Court with business owners seeking relief against defamatory online reviews, including court orders to identify anonymous reviewers.

Until very recently, recipients of an anonymous negative online were generally powerless against the cloaked complainer, with the only real option to respond to the review and hope that no one would pay it any attention. It's a David and Goliath story; in one corner, the helpless business owner with just a slingshot to defend its reputation. In the other corner, the multinational tech giant backed by an army of keyboard warriors brandishing (s)words.

Just two years ago, the High Court paved the way for defamation proceedings against search engines in the landmark case *Trkulja v Google Inc [2018] HCA 25*. Since 2018, the significance of and reliance upon online reviews has accelerated profoundly, with customers turning their nose up at anything less than a 4 out of 5-star rating (or strictly 4.3 and up if you consider yourself a foodie). In the age of Google reviews, customers wield more power than ever before, holding equipped with the weaponry to destroy a business' reputation in 100 characters or less.

The pursuit of defamation proceedings in respect of online reviews has one key barrier: the protection of virtual anonymity. Without the identity of the potential respondent, defamed personnel are unable to commence proceedings. Four successive claims made their way to the Federal Court in February and March this year that herald a strengthened position for besmirched proprietors by lifting the veil of anonymity. This article will examine the recent timeline of online review defamation cases to suggest potential judicial trends towards compelling discovery to identify anonymous online reviewers.

But first, when is a Google review defamatory?

Generally, an action in civil defamation must establish three components: publication, identification and a defamatory meaning. A Google review passes the first two stages by its very nature: a review is published to more than one person other than the party allegedly defamed (i.e. the entire world) and it identifies the allegedly defamed person by naming them or their business. A review will be considered defamatory to the 'ordinary, reasonable person' if it is likely to damage the person's professional reputation by suggesting a lack of qualifications or skills in that person's trade or business. Again, this is often easily established by the brazen nature of a vindictive online review. The potential statutory defences that may be raised in response to a defamatory online review are that of truth and honest opinion:

1. **Truth:** If the claim/s made in the Google review are substantially true, there is a complete defence to allegations.
2. **Honest Opinion**: If the author of the review held an honest opinion based on truth and posted such opinion in the form of the review, they will have a full defence regardless of whether that opinion was correct.

1. Damages for defamed Barrister: *Cheng v Lok [2020] SASC 14*

The first major development in Google review defamation litigation occurred on 6 February 2020, when the Supreme Court of South Australia awarded a lawyer a whopping $750,000 in damages against a woman who posted defamatory comments on the firm's *Google My Business* page.

Gordon Cheng was a barrister originally admitted to practise as a lawyer in Hong Kong. Most of his client base was from the Chinese community in South Australia and were referred by word of mouth. The defendant, Isabel Lok, was never a client of Cheng and had never had contact with Cheng. In late February 2019, Cheng discovered a one-star review about his practice posted by Lok which warned clients to stay clear and claimed that Cheng lacked professionalism, gave false and misleading advice and convinced clients to go to court even if their case lacked merit. From late 2019 to February 2019, Cheng gave evidence that he had lost about 80% of his client base while data from Google showed the post had been viewed thousands of times. On 12 March 2019, Cheng posted a concerns notice in response to the review and lodged a complaint with Google. Google deleted the post but Lok continued to post new posts under varied pseudonyms, including her own father's name.

Damages, including aggravated damages, were apportioned by the Court for past and future economic loss, loss of goodwill as well as general damages "to signal the public vindication of [his] reputation." While the motive of the defendant was not revealed in proceedings, their pseudonym-shifting method was transparent.

Unlike the three scenarios examined below, this case fits squarely into the defamation case cookie-cutter with an identifiable respondent.

The waters become murkier when Google is less compliant, and the defamed party is unable to identify the anonymous reviewer. The cases below suggest a trend of preliminary discovery in these circumstances.

2. Dentist won't be mouthed off: *Kabbabe v Google LLC [2020] FCA 126*

Most patients are aware of the unwritten dental code: never speak while someone is operating sharp instruments in your mouth. One anonymous 'patient' chose to speak later, via the protected platform of Google review.

In November 2019, an unknown reviewer under the pseudonym 'CBsm 23' posted a very unfavourable Google review of Dr Matthew Kabbabe's dental clinic. The review described a procedure performed by Dr Kabbabe as "extremely awkward and uncomfortable", a "complete waste of time", not "done properly" and claimed that it seemed like the dentist "had never done this before".

Google declined to take down the review upon Kabbabe's initial request. Kabbabe sent a follow up email to Google seeking any identifying information about user CBsm 23 for the purposes of bringing a defamation action against that user. Google responded saying it would not remove the review and did not have any means to investigate where or when the user ID was created.

On 12 February 2020, Federal Court Justice Bernard Murphy ordered Google to provide Matthew Kabbabe with preliminary discovery of all documents '*relating to the description of an unknown person who posted an allegedly defamatory review in relation to Dr Kabbabe's dental practice on Google.*' The grant of preliminary discovery pursuant to rule 7.22(1) of the Federal Court Rules provides that 'a prospective applicant may apply to the Court for an order to require a party to provide information about a prospective applicant where a person is unable to commence a proceeding because of a lack of information about a party'. Murphy J held that if Kabbabe received access to Google's information regarding the identity of CBsm 23, he may be able to bring proceedings to argue that the review "tended to lower his reputation as a dental surgeon in the opinion of right-thinking members of the community."

In granting the order, Murphy J compelled Google to provide Kabbabe with any identifying information it had control over, including the subscriber information for CBsm 23's account, name of the account user, phone number, IP address, location metadata associated with that account and any other Google accounts which may have originated from the same IP address during a similar time period to when their account was accessed to post the offending review. The Court found that Kabbabe made reasonable inquiries and took steps reasonably required to ascertain the identity of the prospective respondent. The grant of preliminary discovery will assist Dr Kabbabe in identifying the anonymous reviewer to bring defamation proceedings against her or him.

3. Barrister gangs up on Google: *Zarah Garde-Wilson v Google*

Barrister Zarah Garde-Wilson, prominent for representing gangland clients in Melbourne, filed an application in the Federal Court on 17 February 2020 to compel Google to provide information about a pseudonymous reviewer claiming to be a former client. The review posted in early February was published under the name Mohamed Ahmed and criticised Garde-Wilson's criminal law firm. Gard-Wilson publicly responded that her firm had never acted for someone with the name 'Mohamed Ahmed' and that she had forwarded the review to the Google investigations team to be removed. She suspected the review, which stated '"Hiring Zara was the most expensive and worst decision I have ever made" was written by a legal competitor. Google did not remove the review from her page despite the request. Following filing of the application, the post was removed.

In a case management hearing on 23 April 2020, Federal Court Justice Bernard Murphy said he was "inclined" to make the preliminary discovery orders sought on the basis that Garde-Wilson submitted further evidence to support her defamation and misleading and deceptive conduct claims against the reviewer. Justice Murphy's inclination toward a grant of preliminary discovery to support potential defamation claims continues the pattern of Federal Court intervention in cases involving anonymous online authors.

4. Boardroom Brothel brings Google to the table: *Boardroom of Melbourne v Google*

On 2 March 2020, the eminent Boardroom of Melbourne brothel in South Melbourne brought a similar action before the Federal Court to compel Google to provide the IP address of a hostile reviewer. The reviews of the brothel are peppered with creative licence (including in their use of grammar): "The place is cheap and dirty ... after meeting 3 ladies only I asked is there any more?" The reviews also direct customers to a nearby competitor. Upon the request of the Boardroom of Melbourne, Google declined to reveal the identity of the reviewer and refused to remove the reviews.

The business owner of Boardroom of Melbourne gave evidence to the Federal Court that a pattern of one-star reviews posted over several months, often immediately after a positive review, contained false information and significantly lowered the business' Google rating. The matter awaits hearing, but if successful it will continue the line of Federal Court orders to assist with identifying potential respondents to defamation proceedings.

Continued on page 6 >

Key Takeaways

The increasing incidence of Google reviews entering the courts in recent times suggests the virtual shield of anonymity may no longer protect spiteful reviewers. The findings in Cheng propound the potential for onerous damages awards where reviews have been proven to seriously damage a business' reputation, when those reviews have no basis. Moreover, the increasing number of successful applications to the court for preliminary discovery to identify Google reviewers suggests an empowered position for defamed persons who find themselves without any remedies beyond the courtroom. In each of the above preliminary discovery cases, the applicants may also use the identification evidence beyond the scope of defamation action. For example, the tort of injurious falsehood may be claimed where the business owner can prove financial loss resulting from false or malicious statements intended to damage a business.

The Court's ruling for preliminary discovery in *Kabbabe* marks an important counterattack for slandered businesses attempting to track down the source of allegedly defamatory Facebook or Google reviews. Yet, legal victory does not come without great cost and highlights a greater tension between data-armed tech platforms protecting user privacy and users who commit foul play hiding behind those protections. The reluctance of tech-giants to handover user information without being legally compelled wrings out court resources. Persisting information imbalances between search engines and business owners remains a key challenge to reputation management online. Once a review has remained online for the amount of time that it takes for the matter to play out in court, the damage to a business' reputation is well and truly cemented. For small business owners, the importance of a good online rating is unavoidable. Online review platforms would be best served to keep matters out of the court by updating policies to remove unequivocally defamatory reviews from anonymous authors. As the balance of power shifts to small businesses to retaliate in the digital battlefield, Google should act quickly before it is beheaded.

A Lesson in Why Not to Sue for Defamation (or, at least, to settle early):

KSMC Holdings Pty Ltd t/as Hubba Bubba Childcare on Haig v Bowden [2020] NSWCA 28 (3 March 2020)

By **Marlia Saunders,** Senior Litigation Counsel, News Corp Australia

No one wins in defamation cases. Sure, successful plaintiffs can be awarded huge sums of money and be "vindicated" by the courts – but there is always the risk of this being overturned on appeal. More often than not, both plaintiffs and defendants are dragged through the mud throughout the course of the proceedings, with every aspect of their lives being simultaneously under the microscope and broadcast to a much broader audience than the original publication.

This was illustrated all too clearly in the recent decision of the NSW Court of Appeal in *KSMC Holdings Pty Ltd t/as Hubba Bubba Childcare on Haig v Bowden* [2020] NSWCA 28 (3 March 2020). At first instance the plaintiff, a young male childcare worker, was awarded $237,970.22 in damages plus costs in a case concerning an email sent by his employer to 35 recipients. Within a year, he went from this remarkable high to losing his case on appeal and being ordered to pay the costs of the defendants for both the first instance proceedings and the appeal. A devastating result for someone just starting out in their career.

In his appeal judgment, Basten JA was scathing. He took a dim view of the trial judge, the case management of the proceedings, the lack of proportionality between the resources expended in the proceedings as compared to the nature of the claim, and the fact the proceedings were pursued at all. His Honour observed:

> *"…on a broader view, the proceedings have been counter-productive, having regard to their proper purposes. The respondent was a young man starting upon a career. A newsletter sent to 35 parents of children who were cared for by the appellants contained a brief reference to the termination of his employment and the reasons for taking that step. If money was his motive in bringing the proceedings, he has failed entirely and is now subject to a heavy obligation to meet the costs of the defendants. However, a careful assessment of the likely award of damages if successful, together with an appreciation of the risk of failure, might cast doubt on his judgment in bringing the proceedings for that purpose.*
>
> *If his primary purpose was to defend his reputation, one immediate effect of the proceedings was to ensure that the comments in the newsletter became available for public consumption. Furthermore, he had to resist the defence that the adverse imputations were true and also, to prove that they were made maliciously. The fact that he succeeded at trial on both relevant defences must tend to sully the reputations of the defendants. Their success on appeal will only partly remedy that stain. Sullying one person's reputation to protect another's is a high cost. The situation is more troubling where the adverse effect on the defendants appears to have been unwarranted."*

The facts

In April 2016, an email was sent on behalf of the childcare centre to 35 parents of children who attended the centre. Under the heading "Staff Updates", the email stated that the plaintiff "is unfortunately no longer with us due to disciplinary reasons", "was not truthful with us regarding his studies and some other issues" and "I felt it was better for him to move on and possibly gain a bit more life experience". When the plaintiff became aware of the email, he commenced proceedings claiming the email gave rise to false and defamatory imputations that he was dishonest; was not truthful with Hubba Bubba Childcare regarding his studies and some other issues; was fired for disciplinary reasons; conducted himself in such a manner that a childcare centre terminated his employment; and is not a fit person to work in childcare.

Levy DCJ found in favour of the plaintiff, dismissing the defendants' defences of truth, qualified privilege and triviality.

The appeal

However, the Court of Appeal overturned the decision at first instance, finding that:

- Levy DCJ erred in finding that the email was not published on an occasion of qualified privilege at common law, in that he conflated the assessment of whether there was a privileged occasion with an assessment of whether material was included in the email which was irrelevant to the occasion of privilege. It was found that the assessment of whether there was an occasion of privilege is an objective question, and should not take into account the subjective purpose of the publisher. The reference by Levy DCJ to a "defence" or "actual or apparent interest" was described as "regrettable", given no such defence exists to a defamation action.

- Parents at a childcare centre have a legitimate interest in knowing about staffing changes and the reasons for those changes, which supported there being an occasion of privilege. It was found that the court should not take a narrow view of whether what was said on an occasion of privilege was strictly in pursuit of the duty or interest. What must be considered is whether the defamatory statements were "sufficiently connected" to the privileged occasion to attract the defence, and it was held that this was the case.
- Levy DCJ erred in finding that the defendants were actuated by malice. The appeal court observed that to establish a predominantly improper motive in publishing the matter complained of is a "heavy onus" - honesty is presumed, and the plaintiff has the onus of negativing it. Proof of ill-will, prejudice, bias, recklessness, lack of belief in truth or some motive other than duty or interest for making the publication is insufficient of itself to establish that malice actuated the publication. The appeal court found that the evidence did not support a finding of malice.
- Even if the qualified privilege defence had failed, the damages award at first instance was "manifestly excessive". The appeal court noted that "There remains an issue in this State about the fundamental approach to damages in defamation cases" in light of the Victorian Court of Appeal's decision in *Bauer Media Pty Ltd v Wilson (No 2)* (2018) 56 VR 674 and that section 34 of the *Defamation Act 2005* (NSW) provides that the Court must ensure "that there is an appropriate and rational relationship between the harm sustained by the plaintiff and the amount of damages awarded". It was held that an award of $40,000 would have been appropriate in this case, and there was no occasion for an award of aggravated damages.

Criticisms

The Court of Appeal was critical of the fact that:

- the trial in the District Court ran for 11 days, an unjustifiable period given the nature of the claim and the amount at stake, particularly given that the case was heard by a judge sitting without a jury;
- the costs of each party must have exceeded the reasonable expectation of damages in the event of success;
- the judge did not order that the parties exchange witness statements prior to the trial. The appeal court observed that it is common practice in defamation proceedings not to exchange statements, but said this is likely to lead to inefficiencies and that the general practice should be reconsidered; and
- there was a delay of almost 11 months between the conclusion of the evidence and the delivery of the judgment, which was unsatisfactory in a case which turned upon the credibility of witnesses giving oral evidence.

Lessons

Practitioners should be alive to the practical consequences of running defamation proceedings to trial and the potential negative impacts on their clients. Putting to one side the inherent risks and uncertain prospects involved in any litigation, defamation cases also carry the risk of further publicity being given to the alleged defamation, additional adverse material being adduced in the course of a truth defence or bad reputation plea, and adverse and critical findings being made by the court in terms of a party's credit.

Defamation proceedings are also extremely expensive and time consuming. It is often said that only the lawyers come out the winners in defamation cases, but in this case where the huge burden of costs now lies on a person barely in his twenties, it will be difficult for even the lawyers to get their pay day.

Profile: Melissa Sequeira, Legal Manager and Company Secretary at ViacomCBS Networks (Pay) ANZ

CLB Co-editor, **Eli Fisher** (Baker McKenzie), chats to **Melissa Sequeira,** about her career and her reflections on this unique time.

ELI FISHER: Hi Melissa, thanks for chatting with us. Where do you work, and can you tell us a little bit about your role in the organisation?

MELISSA SEQUEIRA: Thanks Eli for the opportunity. I currently work as Legal Manager and Company Secretary for ViacomCBS Networks (Pay) Australia and New Zealand. My role involves providing commercially driven legal and regulatory advice to ViacomCBS brands Nickelodeon, Nick Jr., MTV, Comedy Central and Spike in Australia and New Zealand across all departments including creative services, programming, digital media, advertising sales and commercial partnerships, technology, business development, consumer products, publicity, marketing, events, finance, research, human resources and channel operations. Working in a small but dynamic team, I am involved in structuring, negotiating, drafting and finalising a broad range of commercial agreements to service these departments. In addition, serving as an officeholder (company secretary) on the subscription television side of the business, has equipped me with knowledge and skills of corporate governance within a leading media organisation. My role has also enabled involvement in external and internal working groups. Externally, I represent the company on the ASTRA Legal & Policy Committee and ASTRA IPTV Committee. Internally, I am on the Cyber Incident Response Team, Nickelodeon Standards & Practices Committee and Workplace Health and Safety Committee. I'm also a Classification Trained Content Assessor under the scheme administered by the Department of Communications and the Arts.

FISHER: Where have you worked previously, and what (apart from it being an obvious dream job) led you to your current role?

SEQUEIRA: I am now an experienced legal advisor, having worked in both private practice and in-house, predominantly within the intellectual property, technology, media and entertainment industry. I was fortunate to work with Lloyd Hart, one of the first lawyers to specialise in entertainment law for the Australian film and television industry, early on in my career. He was born into a legal family and his father was a Supreme Court judge in Queensland. Lloyd retired in 2015 after nearly 45 years of dedicated service to the industry. I also worked with Caroline Verge at Verge Whitford & Co Lawyers, a leading film, television and digital media lawyer representing clients engaged in high quality projects. Both were incredibly valuable mentors and instilled in me a passion for working within the creative industries and how to do so with great humility. Throughout my career, I have worked in-house at the Australian Broadcasting Corporation (ABC), along with The Wiggles, before joining the Studio 100 Group (Flying Bark Productions). It was my mentor, who I met through the Communications Entertainment and Technology (CET) Committee, that sent me the role advertisement for Viacom (now ViacomCBS). The position was an exciting next step which has fostered strong commercial legal acumen over the last five years that I've been there.

FISHER: What do you wish you had known about the legal profession before becoming a lawyer? What are some tips for young lawyers looking to work in this area of law?

SEQUEIRA: The difference between litigation and transactional work! Don't believe everything you see on television. Courtroom drama is not the norm! Even working at a media organisation, often on commercial transactions, the majority of my day is in an office environment and it is not particularly glamorous to sit or stand behind a desk and draft contracts. Nonetheless, I love my role and am privileged to attend a variety of events, production shoots and film screenings. In all seriousness, the reality of practising law hasn't been that far away from my expectations and initial perceptions though. Ultimately, my desire to practise as a lawyer was driven by my passion for justice along with helping others solve their problems, which was a dream that has turned into reality. As a solutions driven individual and with the volume of teams I assist daily in-house (and even previously the range of clients in private practice I worked with), I can certainly tick the box of serving others in a commercial environment.

Take advantage of internships and volunteer placements as early as possible in your career. I did an ABC Legal internship in my third year of my combined law degree. Get involved in as many industry committees as possible. A senior lawyer mentioned to me 'I don't care what anyone says, networking is work' and it really resonated for me. Invest time and effort in it for as long as you practise – after all, at the core of everything we do is a social construct. Don't forget to pay it forward to the next generation when you get admitted and experienced

as a lawyer. Be tenacious, be curious and be continually engaged. Get as much experience in the world (maturity helps you negotiate commercial transactions). From 2012-13, I worked in Angers, France teaching English to high school students through a French Embassy of Australia program. It provided me the opportunity to thoroughly improve my French language skills. Balance is also key. Outside of work, you will find me playing electric guitar, running, doing yoga, cooking new creations, painting and socialising with friends.

FISHER: What is a typical day at the office like for you?

SEQUEIRA: Working in-house at a media organisation is extremely varied and I'm involved in a multitude of tasks as I business partner with the brand teams daily – constantly balancing risk without compromising legal integrity. From providing legal advice across the company to drafting contracts, to completing compliance paperwork and advising on advertising regulations, there is no typical day and that's what I thrive on. Each day is a constant re-prioritisation of tasks according to the opportunity, risk and value it offers the organisation at large. Working with international counterparts also means our team has to be continually agile and responsive in this fast-paced environment.

FISHER: What do you consider to be some of the most interesting and challenging aspects of your role?

SEQUEIRA: The nature of the media environment is thoroughly enjoyable for me to practise as a lawyer in. I'm involved in cutting edge work on new media and platforms, innovating with the organisation as it adapts to emerging trends and focused audience research. For example, Nickelodeon has recently launched a 'Do Not Touch' augmented reality app. I am a strong advocate for commercial legal outcomes to flourish through a plurality of opinion. I enjoy collaborating with creative service colleagues when discussing projects and campaigns as they have a unique approach to problem solving. They have taught me to think creatively as a lawyer and to frequently innovate. It's a very progressive environment.

There are challenges due to the volume and speed at which tasks move, which our department constantly navigates. Being an in-house counsel does not afford you the opportunity to sink your teeth deeper into some legal issues you could otherwise get immersed in if it was your sole focus. However, the benefit is that you acquire knowledge of a vast array of practice areas within the business and become very versatile.

FISHER: Across the ViacomCBS family, is there one particular character or show that is a clear favourite of yours (there are no right answers to this, it's completely subjective - except the right answer obviously and objectively involves a blue dog that solves mysteries by finding clues)?

SEQUEIRA: Oh, I'm glad you mentioned that – as a child, I recall watching Nickelodeon's 'Blue's Clues', an animated television series, but it has recently been reimagined as 'Blue's Clues & You!', a live-action/ computer animated television series with a new host, Joshua Dela Cruz. A clear favourite for the children of those who grew up with the program. While I do love solving those mysteries, I can't go past the SpongeBob SquarePants character, my beloved underwater friend, who has featured in numerous projects of mine, from pop-up channels, to the 'Junior Citizens of the Reef' campaign to the Sydney Royal Easter Show float. He turned 20 last year and is still going strong.

FISHER: What are some trends that you are seeing in the media and entertainment industry that will have the most impact on the way the business operates going forward? What are some of the most urgent challenges for the Australian media landscape, and do they differ from those in other Western democracies?

SEQUEIRA: Firstly, the proliferation of subscription video-on-demand (SVOD) providers globally has exerted enormous pressures on media incumbents to compete and survive, or frankly, perish. These SVOD services provide a unique offering to voracious viewers to consume content wherever, whenever and at a desirable price point.

In Australia alone we are serviced by a vast array of SVOD platforms including 10 All Access (ViacomCBS), Netflix, Amazon Prime, Stan, Disney +, Apple TV +, Hayu, Foxtel Now, Kayo and more recently, Binge, with the number of platforms available expected to increase in the next 1-2 years. ACMA's Communications Report 2018-19 demonstrated over 70% of Australians with a home television set used at least 1 paid video streaming service in 2019 and 1 in 10 had 4 or more subscription services in the home in 2019, up from 4% in 2017. Time will tell which platforms have the stamina and pockets to see this contest through. Media players have really had to diversify their operations. Moving forward, I predict companies will continue to leverage platforms and technologies to drive audience engagement, emerging where their audience is.

Secondly, the ACCC Digital Platforms Inquiry (DPI) unwrapped the significant effects of media behemoths like Facebook and Google on competition in Australian media and advertising service markets. The recent Options Paper on Australian Content, a by-product of the DPI review, was commissioned by ACMA and Screen Australia. Here, there appears to be further recognition that media is tangibly converging and I'm sensing a real appetite for relevant change with various models proposed in the Paper, majority of which are outcomes driven for Australian audiences. Deregulation of the Australian content industry with a focus on production incentives and continual Australian Government support will promote freedom of competition, increased creativity and agility, resulting in a thriving and more globally competitive Australian production ecosystem, along with efficiencies for all media businesses. Over the years, my experience with the offsets, particularly the Producer Offset and associated requirements, necessitates significant reform to yield an even playing field in the Australian media industry.

On challenges, continually addressing digital disruption is an urgent issue for the Australian media landscape, but is also having common effects globally, particularly Western Democracies, with countries affected to fluctuating degrees and adopting various regulatory responses. Piracy, for example, is a constant global challenge exacerbated by digital disruption for players. Fundamentally, I see disruption as presenting an exciting and challenging opportunity for companies to redefine the value chain, with those responding at scale and confidently, in a way that's completely embedded in commercial strategy, best positioned to emerge successfully.

While it was a positive step in the right direction when the Government announced its 2017 media reform package, there is still much more to be achieved. Compared to other Western democracies, Australia has an extremely high concentration of media ownership, significantly stifling plurality of views. Pressures around digital disruption are accelerating the merging of media businesses as they attempt to become stronger together.

I'd like to see the modernisation of restrictive and unworkable Australian defamation laws by striking the right balance between reputation and freedom of speech. There's no denying Australia has earned a reputation for being the defamation capital of the world. We could urgently benefit from borrowing concepts from the UK to reform our legislation, like the 'serious harm' test and single publication rule, along with finding positive ways to fall into step with the realities of publishing in the social media digital age. I understand some media outlets are considering an appeal to the High Court following the recent Dylan Voller Facebook case, which imposes liability for media publishers.

I'm also looking forward to the outcome of the inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press.

FISHER: Does the legal status quo enable you to overcome these challenges? If the law reform genie granted you one wish, what would it be?

SEQUEIRA: Definitely not – significant reform is required to create a sustainable screen industry and competitive Australian media industry. As most people would wish for, of course (!), the *Broadcasting Services Act 1992 (Cth) (BSA)* is more than ripe for a complete overhaul and I would love to see that legislation significantly revised. The Australian Government has demonstrated that it has the impetus and is quick to move in cracking down on violent videos on social media, when responding to the 2019 Christchurch attacks. Regarding the *Electronic Transactions Act 2000 (NSW)*, the NSW Government also moved extremely swiftly in response to COVID-19, to allow video conferencing technology like Skype and Zoom to be used in witnessing important legal documents. I would really like to see the Government move rapidly to now stir reform with the BSA.

FISHER: How has COVID-19 affected the industry and your role?

SEQUEIRA: COVID-19 has further exacerbated the already challenged media and entertainment industry, wreaking widespread havoc through the significant decline in advertising revenue, suspension of live sports and the shutdown of licensed venues. Nonetheless, like most industries, we have grown stronger 'together apart'. It was refreshing to see the formation of the Australian Screen Sector Task Force, comprised of leading Australian production companies and screen agencies. This industry working group developed a set of COVID-Safe Guidelines in May, a live document to assist productions and production companies to safeguard their cast and crew by risk mitigation. While physical distancing, increased hygiene practices and limitations on personnel numbers make producing content increasingly difficult in this COVID-19 era, I am cautiously optimistic the media and entertainment industry will bounce back with vengeance, innovate (which is what they do best!) and imaginatively find exciting ways to reach their audiences.

ViacomCBS implemented a working from home policy early in the pandemic and we were swiftly equipped to continue our roles from the comfort of our homes. Work life shifted from creatives at my office desk to constant home video calls on Microsoft Teams, along with remote execution of agreements. The speed at which our company moves did not change and I've continued to service the brand teams from a distance. Fortunately, being a lawyer is an occupation you can perform remotely. As most other lawyers would agree, it can be difficult to implement boundaries when working from home and the days can sometimes blur into one, without being punctuated by a daily routine of attending the office. Until there's a cure and/or treatment for COVID-19, work life as we knew it will never quite be the same.

FISHER: Thanks Melissa! On behalf of all our readers, we are really grateful for your insights. (Seriously, what do I have to do to get some Blue's Clues merch "for the kids"?)

SEQUEIRA: Haha, I'll see what I can do…for the kids, of course.

All views expressed are my own.

Eli Fisher, co-editor, is a Senior Associate at Baker McKenzie.

Injurious Falsehood and the Fine Line Between Colourful Language and Malice:

Omega Plumbing Pty Ltd v Harbour Radio Pty Ltd t/as 2GB and 2GB 873 [2019] NSWSC 1576

Adaena Sinclair-Blakemore, Associate, Baker McKenzie, discusses the recent *Omega Plumbing v Harbour Radio judgment,* relating to establishing malice in injurious falsehood proceedings.

1 Introduction

When does a shock jock's colourful language cross the line between free speech to malicious conduct? This question was recently addressed by the Supreme Court of New South Wales in an application for an interlocutory injunction in *Omega Plumbing v Harbour Radio Pty Ltd t/as 2GB and 2GB 873* [2019] NSWSC 1576.

Omega Plumbing Pty Ltd (**Omega**) brought proceedings against the shock jock radio host Ray Hadley and his broadcaster 2GB for injurious falsehood in respect of comments made by Hadley and published by 2GB about Omega. Omega sought an interlocutory injunction to prevent further publication pending the final hearing in the proceedings. Although Justice Davies found in favour of Omega, the decision nevertheless provides a timely reminder of the difficulty faced by plaintiffs in succeeding on a claim for injurious falsehood given the high burden imposed upon plaintiffs to prove that a defendant acted maliciously.

2 Injurious falsehood

The tort of injurious falsehood seeks to protect a plaintiff's economic interests that have been damaged by false statements made maliciously.[1] There are four elements that a plaintiff must prove in order to succeed:

1. that false statements were made by the defendant;
2. that those false statements were published;
3. that those false statements were made maliciously; and
4. that the plaintiff has suffered actual loss.

Injurious falsehood is a similar cause of action to defamation but there are some distinct differences between the two, most notably the requirement to prove malice, which may be the most contentious element of the cause of action.[2]

"Malice" in the context of injurious falsehood is not easy to precisely define and there is no bright line delineating when false statements will or will not have been made maliciously.[3] The key principles from the long line of case law are that:

- where a defendant has actual knowledge of the falsity of a statement this will be sufficient to show malice (however, it is often very difficult to prove actual knowledge of the falsity of the statement);[4]
- recklessness is not sufficient in and of itself to amount to malice. However, reckless indifference as to the truth in a way that amounts to wilful blindness will amount to malice;[5]
- mere carelessness or lack of a positive belief in the truth is insufficient to amount to malice;[6] and
- malice is generally inferred from conduct and words of the defendant and the "grossness and falsity of the assertions and the cavalier way in which they were expressed".[7]

3 Facts of the case

Over the course of four days, between 29 October 2019 and 1 November 2019, Hadley made numerous statements about Omega, an emergency plumbing company that operates in the Greater Sydney area, in response to a limited number of complaints that Hadley had received from his listeners about Omega on his radio show. Hadley's broadcaster, 2GB, published these comments on air and in articles on its website. The table on page 13 provides the key statements that Justice Davies focussed on in the decision.

4 Decision

The defendants did not challenge that there was a prima facie case that the statements were false and that Omega had suffered actual loss,[8] so the decision turned on whether the statements were made by the defendants maliciously.

1 *Ballina Shire Council v Ringland* (1994) 33 NSWLR 680 at 694 (Gleeson CJ).
2 See, eg, *Palmer Bruyn & Parker Pty Ltd v Parsons* (2001) 208 CLR 388 at 419-20 (Kirby J).
3 *Schindler Lifts Australia Pty Ltd v Debelak* (1989) 89 ALR 275, 291 (Pincus J).
4 *Horrocks v Lowe* [1974] 1 All ER 662, 669 (Lord Diplock) cited in *Omega Plumbing v Harbour Radio Pty Ltd t/as 2GB and 2GB 873* [2019] NSWSC 1576 at [18].
5 *Schindler Lifts Australia Pty Ltd v Debelak* (1989) 89 ALR 275, 291 (Pincus J).
6 *Roberts v Bass* (2002) 212 CLR 1, 31.
7 *AMI Australia Holdings Pty Ltd v Fairfax Media Publications Pty Ltd* [2010] NSWSC 1395 at [32], citing *Joyce v Sengupta* [1993] 1 All ER 897, 905-6.
8 *Omega Plumbing v Harbour Radio Pty Ltd t/as 2GB and 2GB 873* [2019] NSWSC 1576 at [16].

Date	Statements made by Ray Hadley and published by 2GB
29 October broadcast	• "they've been excluded from the [Master Plumbers] Association for a long period of time, apparently" • quoted a representative of Omega who denied any wrongdoing: "Our business is primarily an emergency response business. This means we regularly have to give our customers bad news, the repair can run to thousands of dollars. This can sometimes be misconstrued."
30 October broadcast	• "anyone that deals with Omega is as mad as a cut snake because they're just like the Plumbing Detectives; they're thieves." • "it's almost verging on extortion" • Omega trades under various names (e.g. Omega Home Services, Omega Plumbing, Omega Drains, Omega Heating and Cooling), to which Hadley commented: "this is done to dupe people"
30 October article	• "Omega is trading under 13 different company names, making it even more difficult to avoid their shonky practices" • "Give them all their money back, because you did bloody nothing … you're just thieves."
31 October broadcast	• "[Omega] preys on immigrant families in wealthy areas who don't have English as their first language" • "[one of my first questions to anyone from Omega would be that] having you in the studio makes my skin crawl"
31 October article	• "Omega Plumbing silences the victims of their rorts" • "Ray Hadley can reveal cowboy plumbers Omega Home Services are coercing dissatisfied customers into non-disclosure agreements"
1 November broadcast	• "Omega actively targets the elderly and affluent immigrant communities"

While Omega could not prove that Hadley and 2GB had actual knowledge of the falsity of the statements made, Justice Davies found that several of the comments did establish a prima facie case of malice because they evinced a reckless indifference as to the truth in a way that amounted to wilful blindness.

First, the Court found that Hadley's assertion that Omega traded under different names "to dupe people" was made maliciously. None of the complaints that Hadley had received from listeners concerned the identity of the company with whom the complainants dealt. The Court found that there was simply no evidence that the use of different business names or companies was designed to mislead consumers, which meant that Hadley's assertion was reckless to such an extent that it made out a prima facie case of malice.[9]

Secondly, Justice Davies took issue with the comment made by Hadley during the 31 October broadcast that the first question to any representative of Omega who came on his program would be how they felt about being a bloke "who duds the elderly and charging them 10, 20 and 30 times more than a job's worth". The Court found that that this statement supported a prima facie case of malice because "there was a complete absence of material to justify its being made", as there was no evidence that Omega had charged anyone, let alone elderly customers, 20 and 30 times more than a job's worth.[10]

Thirdly, there was the allegation made on a number of occasions that the plaintiff "preys" upon elderly people and affluent migrant communities. Justice Davies observed that while two of the complainants who expressed their concerns about Omega were elderly, this was "entirely different" to and fell far short of there being any evidence to justify that this amounted to "targeting" these groups of people.[11]

Finally, a significant aspect of Justice Davies' consideration of the submissions regarding malice is that his Honour accepted Omega's argument that malice may be proved from conduct over a period of time and not from only one instance or statement.[12] While his Honour

9 *Omega Plumbing v Harbour Radio Pty Ltd t/as 2GB and 2GB 873* [2019] NSWSC 1576 at [45].
10 *Omega Plumbing v Harbour Radio Pty Ltd t/as 2GB and 2GB 873* [2019] NSWSC 1576 at [46].
11 *Omega Plumbing v Harbour Radio Pty Ltd t/as 2GB and 2GB 873* [2019] NSWSC 1576 at [48].
12 *Omega Plumbing v Harbour Radio Pty Ltd t/as 2GB and 2GB 873* [2019] NSWSC 1576 at [50]-[51].

accepted the defendants' submission that returning to the same subject-matter over the course of several days is not in itself any evidence of malice, his Honour noted the "more balanced" tone used by Hadley during his first broadcast on 29 October 2019, in which he read aloud a statement provided by Omega, with the escalation of the language used in the following days, such as "thieves"; "extortion"; "dupe people"; "preys on the elderly"; "having you in the studio makes my skin crawl"; and "making millions by targeting the elderly and immigrants". The Court again noted that it is relevant to consider the "grossness and falsity of the assertions but also the cavalier way in which they were expressed".[13]

Justice Davies granted the plaintiff's request for an interlocutory injunction pending the final determination of the proceedings.

5 Implications and conclusions

This decision is noteworthy for several reasons. First, it is a timely reminder of the difficulties faced by a plaintiff in succeeding in a claim of injurious falsehood given the high threshold to be met to prove malice on the part of a defendant. This is a significant hurdle for plaintiffs who have been economically affected by false statements made by a defendant, particularly where the plaintiff is a business with more than ten employees. This is because businesses with more than ten employees cannot bring claims for defamation, for which malice need not be proved,[14] and are therefore limited to bringing claims in injurious falsehood.

Secondly, the case nevertheless demonstrates that there are limits to the way in which a talkback radio host or any other broadcaster can express their views, particularly when basing those views on unconfirmed complaints received by listeners. Furthermore, radio hosts and broadcasters should note Justice Davies' focus on the repetition of the statements and the escalation of the language used over the relevant time period.

13 *Omega Plumbing v Harbour Radio Pty Ltd t/ as 2GB and 2GB 873* [2019] NSWSC 1576 at [51] (citing Brereton J's remarks in *AMI Australia Holdings Pty Ltd v Fairfax Media Publications Pty Ltd* [2010] NSWSC 1395 at [32]).

14 *Defamation Act 2005* (Vic) s 9(2); *Defamation Act 2005* (NSW) s 9(2)(b).

Contributions & Comments

Contibutions and Comments are sought from the members and non-members of CAMLA, including features, articles, and case notes. Suggestions and comments on the content and format of the Communications Law Bulletin are also welcomed.

Contributions in electronic format and comments should be forwarded to the editors of the Communications Law Bulletin at: **clbeditors@gmail.com**

Smethurst v Commissioner of Police [2020] HCA 14: Case note

Will Sharpe, Partner, HWL Ebsworth, summarises and comments on the *Smethurst v Commissioner of Police* decision, in which the High Court weighs up confidentiality, privacy and public interest considerations in refusing an order for destruction of material seized under warrant.

In *Smethurst v Commissioner of Police* [2020] HCA 14, the High Court considered the validity of a search warrant under which material was taken from News Corp journalist Annika Smethurst during a search of her home, and, if invalid, whether an order should be made for the destruction of the documents. Ms Smethurst was successful in establishing that the warrant was invalid, but not in obtaining an order for the destruction of the documents.

On the question of the destruction of the documents, the Court split 4:3 in favour of permitting the AFP to retain the documents seized for the purposes of its investigation. The case raised various questions relating to confidentiality and privacy of information, and the public interest associated with the investigation of possible crimes.

The warrant is found to be invalid

In a joint decision, Kiefel CJ, Bell and Keane JJ explained that the terms of the warrant were not consistent with the requirement that a warrant state the particular offence to which it relates. The warrant had sought to summarise the offence in question, but in doing so both failed to state the nature of the offence, and 'succeeded in misstating it' (at [43]).

The need for a warrant to state the offence to which it relates has its history in the law's refusal to accept 'general warrants' that confer a 'free-ranging power of search' (at [22]). The requirement now has a statutory basis in the *Crimes Act 1914* (Cth) (the Crimes Act). The 'protective purpose' of the requirement, their Honours explained, is achieved 'by ensuring that each of the issuing officer, the officer executing the warrant and the persons affected by the warrant understand what is the object of the search and the limits to it' (at [27]).

In the case of the warrant for the search of Ms Smethurst's home, their Honours said (at [43]):

Those reading the warrant were not only uninformed about any offence under s 79(3) [of the Crimes Act], they were misinformed that the offence concerned the provision of a document to another person which was somehow said not to be in the interest of the Commonwealth.

That meant that '[i]t is not immediately apparent how [Ms Smethurst] and the executing officer were to understand the boundaries of the search .... It made the authorisation for the search appear impossibly wide' (at [43]).

The remaining members of the Court (Gageler, Nettle, Gordon, and Edelman JJ) each delivered separate judgments, but agreed with the plurality that the search warrant was invalid.

Why did the court not require the destruction of the seized material?

The question that split the Court was in relation to the injunction sought by Ms Smethurst that would have required that the AFP either destroy or deliver up the information taken from her mobile phone, or restrain the AFP from making the information available to the prosecutor.

Justices Gageler, Gordon, and Edelman would have granted the injunction sought by Ms Smethurst, but would have framed the injunction in a way that would have allowed the AFP to attempt to obtain a lawful warrant to allow them to retain the seized information.

At issue was confidentiality, privacy, infringement of common law rights by trespass, public interest considerations relating to the administration of justice and investigation of a possible crime, and the scope of the Court's jurisdiction to grant an injunction.

The court did not determine whether there is a common law right to privacy

First, for those interested in the possible recognition of a common law right to privacy, or a tort for invasion of privacy, Ms Smethurst did not seek to claim such a right or the existence of such a tort (at [48]). The Court, therefore, did not delve into the question left open by *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199. There were hints, however, that this is an issue that the Court would be interested in returning to in the future (see, for instance, [86] – [90]).

Seized material is not confidential information recognised by the law

Neither did Ms Smethurst claim that the information seized was in the nature of confidential information that would of itself support the grant of an injunction on equitable grounds. Although the information may have been confidential in the sense that it could not be readily accessed by anyone else, it was not claimed to be information that was 'improperly or surreptitiously obtained' (at [47]). (Elsewhere, it has been said that equity will also restrain the publication of information that has the 'necessary quality of confidentiality'—in that it is not common or public knowledge—was received in circumstances to import an obligation of confidence, and there

is actual or threatened misuse of the information (see *Smith Kline & French Laboratories (Aust) Limited v Secretary, Department of Community Services and Health* (1990) 22 FCR 73, at 87).)

Should the injunction be issued to respond to the trespass committed by the AFP?

The claim for the injunction was instead sought to protect against the effects of the trespass committed against Ms Smethurst.

Keifel CJ, Bell and Keane JJ did not agree that the injunction was able to issue on those grounds, largely because, in their view, Ms Smethurst had not suffered damage by the taking of the information (despite acknowledging it may have serious consequences for her) (at [72]). It is not possible, they said, 'to regard the prospect that one may be investigated for an offence as injury' (at [73]). Ultimately, they found that Ms Smethurst could point to 'no authority which recognises their interest in not being investigated in relation to an offence as a right' (at [85]).

Even if the grant of an injunction could be made, their Honours took the view that it should not. They said that the public interest in both the investigation and the prosecution of crime meant that the grant of the injunction was not appropriate, and the prospect that criminal conduct may be disclosed was a sufficient reason to decline the relief Ms Smethurst sought (at [104]).

Their Honours also noted that there is no presumption in law that information unlawfully obtained cannot be used in the investigation or prosecution of an offence. There is instead, a public interest in bringing persons to conviction, and this is to be weighed by a court against approving unlawful conduct (at [65]). Their Honours appear to have taken the view that the appropriate time for that weighing exercise is at the point that the information obtained in reliance upon the unlawful warrant is sought to be used in any proceedings against Ms Smethurst for the prosecution of an offence.

On the other hand, Gageler J found that the trespass committed by the AFP, the 'serious and ongoing' effect as long as the information remains in the hands of the AFP (at [122]), and the need to restore Ms Smethurst to the position she would have been in if her common law rights had 'not been invaded by the tortious conduct of the AFP' (at [130]), provided the basis for an injunction to be granted. And, in the circumstances, the AFP could not establish that the discretion should be exercised to refuse the injunction (at [134] – [138]).

Similarly, Edelman J saw trespass, and the 'ongoing and very serious' damage caused by the trespass, as the basis for the issue of an injunction to require that the seized material be delivered up to Ms Smethurst (see [246], [251] and [252]). However, in deciding that the injunction should be given, his Honour also weighed up the fact that the information seized from Ms Smethurst was private information, and because it was not seized under a lawful warrant, it was not subject to the protections that would have applied under the Crimes Act (at [263]).

Should injunction be available to protect against excess of power?

Justice Gordon saw a different basis for the grant of an injunction, and one that was not reliant upon establishing a freestanding right on the part of Ms Smethurst to have the seized material destroyed. It was not necessary, therefore, in her Honour's view for Ms Smethurst to rely upon trespass as a basis to be granted the injunction. Instead, the grant of the injunction was founded on the principle that officers of the Commonwealth must obey the law, and there needs to be effective remedies when they exceed their powers (at [169]; also see [176], [179], [183], [185], and [187]).

This approach to the availability of injunction as a remedy would expand the role of s.75(v) of the Constitution. Justice Gordon summarised the approach by stating that, the constitutional purpose of s.75(v) (and Part IV of the *Judiciary Act 1903* (Cth)) point to the High Court having the power to 'grant all such remedies … as will not only prevent excess of federal power but will also, when federal power has been exceeded, restore the parties affected, so far as possible, to the position in which they would have been had power not been exceeded' (at [182]). Hence, in her Honour's view, the grant of an injunction is not limited to where it is necessary to prevent the implementation of invalid exercises of power (compare Kiefel CJ, Bell and Keane J at [96]), and it was not necessary to identify (as Gageler and Edelman JJ did) a legal right that has been infringed.

Takeaways

- Courts will carefully scrutinise exercises of powers that permit intrusion into a person's private affairs.
- However, the law also recognises competing public interest considerations.
- In this case, it was the failure to comply with the protective requirements of the Crimes Act that caused the search warrant to be invalid, rather than the nature of the information that was seized.
- The Court also recognised that there is a public interest in allowing information obtained without authority to be used in the investigation and prosecution of an offence.
- The law does not recognise all privately held information to be confidential.
- Although it was not called on in this case to consider the existence of a common law right to privacy, the High Court has shown an interest in addressing this issue in the future.

OAIC v Facebook

Katherine Sainty, Principal and **Belyndy Rowe,** Senior Associate at Sainty Law discuss the Privacy Commissioner's claim against Facebook in relation to Cambridge Analytica.

The Australian Information Commissioner (**Commissioner**) has been granted leave by the Federal Court of Australia to serve legal documents on US-based Facebook Inc and Facebook Ireland.[1] The Commissioner brought proceedings against the Facebook entities in the Federal Court in March this year, alleging the social media platform has committed 'serious and/or repeated interferences' with privacy in contravention of Australian privacy law.[2]

1. Background to claim

The Commissioner's claim relates to the Cambridge Analytica revelations of March 2018. To recap, Facebook is alleged to have shared the data of more than 300,000 Australians with British firm Cambridge Analytica through the personality quiz application *'This is Your Digital Life'* (**App**). Cambridge Analytica was caught boasting that it used the data harvested from Facebook user profiles to target political advertising and affect the outcome of the 2016 US Presidential election.[3]

At the time of the Cambridge Analytica breach, Facebook said the data of 311,127 Australians was shared with the App between March 2014 and May 2015, accounting for 0.4% of users affected by the breach worldwide.[4] However, the OAIC's Statement of Claim says only around 53 people in Australia actually installed the app.[5] This demonstrates the reach of the App, which collected not only the data of people who installed it, but also 'friends' in their Facebook network.

The Commissioner's move against Facebook follows action already taken by its international counterparts. Facebook was fined £500,000 by the UK data protection regulator, Cambridge Analytica and Facebook's Mark Zuckerberg received a congressional grilling in the US, and Facebook paid $US5 billion following an investigation by the US Federal Trade Commission over allegations it 'deceived' users about their ability to control their personal information.[6] The Commissioner's claim marks the first attempt in Australia to seek civil penalties through the Federal Court for contraventions of the *Privacy Act 1988* (Cth) (**Privacy Act**).

2. The Commissioner's claim

The Commissioner alleges that Facebook disclosed the personal and sensitive information of Australian Facebook users to the App during the period 12 March 2014 to 1 May 2015. The Commissioner argues this amounted to serious and/or repeated interferences with the privacy of the Australian users, in contravention of s13G of the Privacy Act.[7]

The Privacy Act establishes the 13 Australian Privacy Principles (**APPs**). These are binding principles that govern the collection, use and disclosure of personal information by businesses (other than small businesses) and agencies operating in Australia.[8] Both of the respondent Facebook entities are subject to Australian privacy laws because they conduct business in Australia, which means they are organisations with an Australian link within the meaning of s 5B(3) of the Privacy Act.[9]

APP 6 Contraventions

The Commissioner alleges that Facebook breached APP 6 by disclosing the users' personal information for a purpose other than that for which it was collected.[10] An APP entity can only use or disclose personal information for a purpose for which it was collected, known as the 'primary purpose', or for a secondary purpose if an exception applies.[11]

Facebook collected the users' personal information for the purpose of enabling those individuals to build an online social network with other users on the Facebook platform. Facebook contravened APP 6 because its disclosure of the personal information of users to the App was not for that same purpose.[12] The Commissioner argues that each separate disclosure constitutes a breach of the Privacy Act.[13]

APP 11 Contraventions

The Commissioner also alleges that Facebook breached APP 11 by failing to take reasonable steps to protect the users' personal information from unauthorised disclosure.[14]

1 *Australian Information Commission v Facebook Inc* [2020] FCA 531; Office of the Australian Information Commissioner, 'Statement on Facebook proceedings' (Statement, 22 April 2020) <https://www.oaic.gov.au/updates/news-and-media/statement-on-facebook-proceedings/>.

2 Australian Information Commissioner, 'Concise Statement', *Australian Information Commissioner v Facebook Inc & Anor*, NSD246/2020, 9 March 2020, [1].

3 Emma Graham-Harrison, Carole Cadwalladr and Hilary Osborne, 'Cambridge Analytica boasts of dirty tricks to swing elections', *The Guardian* (online), 20 March 2018 <https://www.theguardian.com/uk-news/2018/mar/19/cambridge-analytica-execs-boast-dirty-tricks-honey-traps-elections>.

4 Josh Taylor, 'Facebook sued by Australian information watchdog over Cambridge Analytica-linked data breach', *The Guardian* (online), 9 March 2020, <https://www.theguardian.com/technology/2020/mar/09/facebook-cambridge-analytica-sued-australian-information-watchdog-300000-privacy-breaches>.

5 Australian Information Commissioner, 'Statement of Claim', *Australian Information Commissioner v Facebook Inc & Anor*, NSD246/2020, 9 March 2020, [45].

6 Information Commissioner's Office, 'Investigation into the use of the data analytics in political campaigning' (11 July 2018), <https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf>; Information Commissioner's Office, 'Notice of Intent', (19 June 2018), <https://ico.org.uk/media/2259364/facebook-noi-redacted.pdf>; United States of America Before the Federal Trade Commission, In the Matter of Cambridge Analytica, LLC, a corporation, Opinion of the Commission, <https://www.ftc.gov/system/files/documents/cases/d09389_comm_final_opinionpublic.pdf>.

7 Australian Information Commissioner, above n 2, [7].

8 *Privacy Act 1988* (Cth) s 28(1) (***Privacy Act***).

9 Australian Information Commissioner, above n 5, [3.5]; *Australian Information Commission v Facebook Inc* [2020] FCA 531, [39] (Thawley J).

10 Australian Information Commissioner, above n 2, [17].

11 *Privacy Act*, sch 1 APP 6.

12 Australian Information Commissioner, above n 2, [17].

13 Ibid, [18].

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure. Where an entity subject to the APPs no longer needs personal information for any purpose for which the information may be used or disclosed under the APPs, the entity must take reasonable steps to destroy the information or ensure that it is de-identified, unless an exemption applies.[15]

The Commissioner alleges Facebook failed to take reasonable steps to protect those individuals' personal information from unauthorised disclosure. In fact, the Commissioner has claimed Facebook did not know the precise nature or extent of the personal information it disclosed to the App, nor did it prevent the app from disclosing the personal information it obtained to third parties.[16] The full extent of the information disclosed, and to whom it was disclosed, is still not known.

Systemic Failures

The Commissioner has described Facebook's breaches of the APPs, and its failure to take steps to prevent the breaches, as 'systemic failures' to comply with Australia's privacy laws.[17] Aside from Facebook's failure to protect personal information from misuse, it alleges Facebook's default settings left users 'unable to exercise consent or control' about how their personal information was disclosed to the App.[18]

To register for a Facebook account, a user was required to accept the Facebook website's Terms of Service (Statement of Rights and Responsibilities) and agree that they had read the Facebook Data Use Policy.[19] The Commissioner's Statement of Claim details the registration process, noting the documents were not located on the user registration page, but located in a separate page accessed via a link, and that registration could be completed without the user viewing either document. To modify their account privacy settings after registering, a user was required to search for settings across multiple screens.[20] In short, privacy by design was not a feature of Facebook's services.

3. Privacy implications

Some commentators have criticised the Commissioner for the length of time taken to launch action against Facebook, given that it commenced its investigation of Facebook over the breach in April 2018.[21] Since then, Facebook has cooperated with international regulators and made changes to its privacy settings and permission controls. Facebook has also taken steps to restrict the information available to app developers.[22]

There are several possible reasons for the Commissioner's timing, including resource constraints and the scope of the investigation. The timing is perhaps not as important as the Commissioner's message to entities operating in Australia. It is clear this behaviour will not be tolerated – even when it concerns big tech.

Implications for entities

The case could provide valuable judicial guidance in an area of law that is rarely litigated and will likely have compliance implications for entities dealing in data and operating in Australia.

The notion that entities are responsible for the personal information they collect and hold is a fundamental principle underpinning the Privacy Act.[23] The Commissioner alleges Facebook failed to take responsibility by allowing third party apps to access data without proper processes in place.

The App operated separately to the Facebook platform and requested data about Facebook users from Facebook, including data from users that did not install the App. At the time, Facebook relied on app developer self-assessments of their compliance with Facebook's policies and procedures, including the terms of the Platform Policy, rather than conducting its own assessments.[24] In doing this, Facebook effectively transferred responsibility for protecting users' personal information to the operators of third party apps.

OAIC's expectations of Facebook in relation to data sharing with third parties is relevant to all entities operating in Australia and sharing personal information under contractual arrangements. The Commissioner expected that Facebook should have, at a minimum, investigated whether the third-party App's requests for Facebook users' information complied with Facebook's own policies, maintained and regularly reviewed a record of the personal information it disclosed to the App, and ensured clear and specific consent was obtained directly from the users.[25]

In May 2014, Facebook found the App did not meet Facebook's updated app requirements and rejected its application to access further information.[26] The Commissioner

14 Ibid, [19].
15 *Privacy Act*, sch 1 APP 11.
16 Australian Information Commissioner, above n 2, [3].
17 Ibid, [26].
18 Ibid, [25].
19 Australian Information Commissioner, above n 5, [11], [13].
20 Australian Information Commissioner, above n 5, [16] – [24].
21 Office of the Australian Information Commissioner, 'Investigation into Facebook Opened' (Statement, 5 April 2018) <https://www.oaic.gov.au/updates/news-and-media/facebook-and-cambridge-analytica/>; Christopher Knaus, 'Australian privacy watchdog fails to deliver findings on Cambridge Analytica scandal after 18 months', *The Guardian* (online), 19 October 2019, <https://www.theguardian.com/australia-news/2019/oct/19/australian-privacy-watchdog-fails-to-deliver-findings-on-cambridge-analytica-scandal-after-18-months>.
22 Facebook, 'Actions We're Taking: Protecting Privacy and Security' (2018) <https://about.fb.com/actions/protecting-privacy-and-security/>.
23 *Privacy Act* 1988 (Cth), sch 1 APP 11.
24 Australian Information Commissioner, above n 5, [36.3].
25 Ibid, [76].
26 Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach', *The Guardian* (online), 18 March 2018 <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.

argues that at this point, Facebook should have reviewed the categories of data the App had previously collected and stopped disclosing the information to the App.[27] The Commissioner alleges that Facebook allowed the App to continue accessing users' personal information for a further 12 months.[28]

Part of the Commissioner's claim focuses on Facebook's failure to take reasonable steps in the circumstances to protect Facebook users' personal information from unauthorised disclosure. Facebook's default settings facilitated the disclosure of personal information, including sensitive information, at the expense of user privacy. Its failure to take proper steps to protect Australians' personal information exposed its users' data to disclosure, monetisation and deployment for political profiling purposes beyond users' reasonable expectations.[29]

The Commissioner alleged that Facebook's disclosure of the personal information of users breached the Privacy Act 'on each occasion' and that Facebook engaged in further breaches of the Privacy Act including by failing to take appropriate security steps. The Federal Court can impose a civil penalty of up to $1.7 million for each serious or repeated interference with privacy, but has never been called to do so.[30] If the Court agrees with the Commissioner, Facebook could be found to have contravened the Act several hundred thousand times. It will be interesting for entities operating in Australia to see how the Court calculates a penalty if it finds against Facebook.

Implications for platform users

Our privacy laws seek to give us the knowledge to make an informed decision about how our data is used. But for customers trading their data for the use of 'free' services like Facebook, breaches such as this make it clear that this cannot be a fair, or even an informed exchange when we are not allowed to see what is being collected from us and for what purpose. This is one of the key points of the Commissioner's claim, which characterises Facebook's actions as a breach of privacy by complexity of terms of use.[31] Facebook's opaque design meant users' ability to understand that their data was being disclosed to the App was diminished.[32]

Facebook has already made changes to the layout of its privacy settings, but the continued use of data collecting methods and corresponding explanations that are not clear and transparent, means consumers remain far from being able to effectively control access to their personal information.[33] The Commissioner has increasingly raised the intersection between privacy and consumer law, and their 'complementary ability to address consumer harm,'[34] and the Australian Competition and Consumer Commission (ACCC) was critical of the privacy practices of digital platforms in the Final Report of the Digital Platforms Inquiry.[35]

The ACCC's report findings and recommendations complement the Commissioner's issues with Facebook. These include criticism of privacy policies as too complex and low on real choices for consumers, and recommendations that notification and consent should be strengthened, disclosures of personal information should be 'fair', unfair contract terms should be prohibited, and individuals should have direct rights of action for breaches.[36] The ACCC is concerned that customers of the platforms are not provided with meaningful control over the use of their data, and the bargains struck between consumers and digital platforms lack bargaining power equality and are unfair.[37]

Alongside *OAIC v Facebook*, we will watch ongoing scrutiny of digital platforms by the ACCC, including the introduction of compulsory fees for Facebook and Google's use of media content, and the ACCC's commencement of an action against Google for allegedly misleading consumers by failing to disclose that their applications may be collecting location information about users irrespective of their settings.[38] This action by ACCC is the first of what could be a series of consumer law actions against the digital platforms for their misleading privacy practices.

4. Conclusion

It is too early to comment on the potential outcome of the litigation, but the fact that the action has commenced is significant. The OAIC wants the Australian public to know that it takes it privacy rights seriously. Making an example of a major international player that has breached Australian law sends this message. The action can also be seen as part of the increasing regulatory pressure on big tech operations in Australia, alongside concurrent work by the ACCC. The continuing rise of digital platforms means that the uses and abuses of platform users' personal data will continue to be a key issue for both privacy and consumer law.

27 Australian Information Commissioner, above n 2, [19].
28 Ibid, [15].
29 Office of the Australian Information Commissioner, 'Commissioner launches Federal Court action against Facebook' (Statement, 9 March 2020) <https://www.oaic.gov.au/updates/news-and-media/commissioner-launches-federal-court-action-against-facebook/>.
30 *Privacy Act 1988* (Cth) s 13G; Office of the Australian Information Commissioner, 'Chapter 6: Civil penalties — serious or repeated interference with privacy and other penalty provisions' (Guide to privacy regulatory action, May 2018), < https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-6-civil-penalties/>.
31 Australian Information Commissioner, above n 2, [25].
32 Ibid.
33 Karim Amer, Jehane Noujaim, 'The Great Hack' (2019), documentary film.
34 Office of the Australian Information Commissioner, 'Privacy implications of the Digital Platforms Inquiry' (Speech 20 November 2019), < https://www.oaic.gov.au/updates/speeches/privacy-implications-of-the-digital-platforms-inquiry/>.
35 Australian Competition and Consumer Commission, *Digital Platforms Inquiry - Final Report*, 26 July 2019, <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf>.
36 Ibid.
37 Australian Competition and Consumer Commission, above n 34.
38 *Australian Competition and Consumer Commission v Google Australia Pty Ltd & Anor*, NSD1760/2019, 29 October 2019.

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
- broadcasting
- copyright
- advertising
- information technology
- freedom of information
- contempt
- privacy
- censorship
- film law
- telecommunications
- 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 $140.00 (includes GST)

☐ Student membership $45.00 (includes GST)
(include undergraduate full time student card copy)

☐ Corporate membership $595.00 (includes GST)
(include a list of names of individuals - maximum 5)

☐ Subscription without membership $150.00
(includes GST) (Library subscribers may obtain extra copies for $10.00 each + GST and handling)