CAMLA COMMUNICATIONS LAW
BULLETIN
Communications & Media Law Association Incorporated
Volume 38, No 3. September 2019
Special Innovation Edition

Defamation Panel:
Voller v Nationwide News Pty Limited; Voller v Fairfax; Voller v Australian News Channel [2019] NSWSC 766

Following a hearing in February this year, the Supreme Court handed down its judgment in the *Voller* case on 24 June 2019, and the result is intriguing for a host of reasons.

For a case this consequential, we've called in a favour (they never owed us anything, but bear with me here) from five of our favourite defamation specialists in the country. This may well be the most ambitious crossover project we have witnessed to date in the CAMLA Universe - expect this to turn into a franchise.

Marlia Saunders is Senior Litigation Counsel at News Corp Australia.
Kevin Lynch is a Media Litigation partner at Johnson Winter & Slattery.
Sophie Dawson is a Media and IT Litigation partner at Bird & Bird.
Robert Todd is a Media and Technology Litigation partner at Ashurst.
Justine Munsie is a Media and IP partner at Addisons.

Eli Fisher: Let's start from the beginning. Who is Dylan Voller, and how does he allege he was defamed?

Kevin Lynch: Mr Voller rose to national prominence after ABC TV Four Corners Program showed confronting footage of him shackled to a restraining chair in the Alice Springs Correctional Centre. The program prompted a Royal Commission into the treatment of youth in the child protection and youth detention systems in the Northern Territory. Mr Voller's history was detailed in the Royal Commission, including repeated terms in custody for a range of crimes including car theft, robbery and assault.

The defamation case is over Facebook "comments", apparently from members of the public, which formed part of the comment feed under links to coverage of Mr Voller variously posted by the Defendants. Whilst the Court is yet to decide whether the publications are defamatory or whether defences arise, I understand that Voller contends that the Facebook "comments" contain baseless allegations of fact - not comment or honest opinion in any defamation sense.

There were four separate proceedings brought by Mr Voller against Australian media companies. The proceedings were filed and served without Voller providing any prior notice of his concerns. One proceeding was resolved early in the piece whilst the action against Nationwide News, Fairfax Media and Australian News Channel proceeded to determination of the preliminary separate question that is the subject of this judgment.

Eli: Can you give us a summary of the judgment?

Sophie Dawson: The Court held that the media organisations which administered Facebook pages (**Page Owners**) were primary publishers of the third party comments.

Contents

CAMLA

Editors
Ashleigh Fehrenbach and Eli Fisher

Editorial Assistant
Imogen Yates

Design | Printing | Distribution
MKR Productions

Editors' Note

Spring has sprung and brought with it the September Special Edition CLB. This special edition on innovation canvasses the latest developments on deepfakes, defamation, artificial intelligence, the implications of 5G's arrival and industry views on press freedom in Australia.

In a novel decision, the Supreme Court of New South has held that media organisations can be liable as publishers of defamatory comments made by third parties on their public Facebook pages. We have collected the insights of leading defamation experts on this landmark decision, **Kevin Lynch**, **Justine Munsie**, **Marlia Saunders**, **Sophie Dawson** and **Robert Todd**.

Artificial intelligence gained more attention from industry bodies this year, in particular with the release of Australian Human Rights Commission's White Paper 'Artificial Intelligence: governance and leadership'. **Paul Kallenbach, Vanessa Mellis, Annabelle Ritchie** and **Siegfried Clarke** (MinterEllison) walk us through the ethical concerns identified in the paper. The MinterEllison team also look at the international developments in the AI space and where Australia sits among these changes. Meanwhile, **Ted Talas** and **Maggie Kearney** from Ashurst dive into efforts to regulate deep fakes and take us through the implications for the Australian legal landscape.

In further news, our representatives from CAMLA Young Lawyers have donned their journalism hats. **Patrick Tyson** from the ABC chats to **Richard Ackland** about press freedom, the recent AFP raids and innovation in the digital news space. **Madeline James** (Corrs) interviews **Matt Collins QC** for his views on freedom of speech, defamation and whether these laws fairly balance the interests of plaintiffs and defendants. HWL Ebsworth's **Amy Campbell** reports on CAMLA's panel discussion on 'Challenges and Opportunities in the Telco Sector' held in August at Bird and Bird.

August also brought to us the 25th rendition of the CAMLA Cup, held once again at Sky Phoenix. CAMLA Young Lawyer representative **Tara Koh** (Addisons) provides us with a report on the well-attended event. A thank you to all attendees of the event – CAMLA looks forward to seeing you again next year! On behalf of CAMLA, we give tremendous thanks to **Deb Richards** (Netflix) and **Ryan Grant** (Baker McKenzie) for hosting the event.

For those eager for more reading material, the ACCC has released its 619-page final report on the **Digital Platforms Inquiry**. Its 23 recommendations have serious implications for the business models of digital platforms and news media businesses in Australia. Whether or not these recommendations will materially affect the value placed on news content remains to be seen. **HealthEngine**, an online health booking platform, has gained attention from the ACCC for sharing personal information with insurance brokers and publishing patient reviews and ratings. **Clive Palmer** is demanding $500,000 from, and threatening to bring a defamation claim against, YouTube creator **FriendlyJordies** for calling him 'Fatty McF--Head' and a 'dense Humpty Dumpty'. Finally, the Federal Court has ordered **Birubi Art,** a seller of fake Indigenous Australian souvenirs, to pay AU$2.3 million in penalties for contraventions of the Australian Consumer Law.

For more, read on.

Eli and Ashleigh

There are two aspects of this decision ("publisher" and "primary") which warrant separate consideration.

In relation to the first question, of whether the Page Owners were "publishers", the Court in *Voller* found that:

- publication of third-party comments to persons other than the Facebook friends of the commenter occurs by virtue of the fact that the owner of a public Facebook page allows access to the comment by the publication of the page; and
- the owner or administrator of a public Facebook page is capable of rendering all or substantially all comments hidden.

On that basis, the Court held that the extended publication of a third-party comment is wholly in the hands of the media company that owns the Facebook page.

The second aspect of this decision concerns whether a Page Owner is a primary or secondary publisher. In short, Justice Rothman said that the Page Owners are primary publishers which means that the defence is not available to them.

Eli: What's the consequence of being classified as a primary (or 'first'), as opposed to secondary (or 'subordinate'), publisher?

Robert Todd: The main consequence is that a primary publisher cannot rely on a defence of innocent dissemination. Secondary publishers can avail themselves of the defence of innocent dissemination if they did not know and could not reasonably have known that the defamatory material had been published or that the published material contained defamatory words. Justice Rothman held that knowledge of the existence of the defamatory material should be presumed not only for primary publishers, but also secondary publishers. However, for secondary publishers the presumption is rebuttable. If a secondary publisher is able to rebut the presumption, they can rely on the innocent dissemination defence, and thereby completely absolve themselves of liability for the publication.

Eli: Can you place this judgment in context? Where are the parties up to in this dispute? What was this judgment addressing, and what was it not addressing?

Justine Munsie: Justice Rothman's judgment addressed a specific question on the preliminary issue of publication – namely, "whether the plaintiff had established the publication element of the cause of action of defamation against the media defendants in respect of each of the Facebook comments by third-party users?"

His Honour's judgment did not deal with the issues of whether the comments were defamatory or whether the media defendants were liable for the comments. The question of whether the defence of innocent dissemination under s 32 of the *Defamation Act* was available to the media defendants was not required to be answered, but given his Honour's finding that they were primary publishers, the issue was touched upon.

Sophie: And to add to what Justine has said, there is some doubt as to whether this second aspect of the decision - that is, whether the Page Owners are primary or secondary publishers - constitutes part of the binding ratio decidendi or whether it is merely obiter.

The judgment is confined to that question that Justine has quoted: whether the plaintiff has established the publication element against the media defendants in respect of the third-party comments.

There is doubt as to whether the above question extends to the plaintiff establishing publication for innocent dissemination purposes, or rather "publication" in the narrower sense. The Court indicated that the parties had at first also framed a question concerning the availability or otherwise of the principle of innocent dissemination. It said that question was withdrawn "perhaps on the basis, to which some authorities refer, that an "innocent disseminator" is not a publisher". The Court also said that "The question on which the parties agreed does not seem, directly, to raise whether the defence of "innocent dissemination", arising under s 32 of the *Defamation Act*, is available. Nevertheless, there are certain aspects of the process by which the comments of third parties are placed, or remain, on the public Facebook page of the defendants that directly raises this aspect".

The drafting of the question and the ambiguity of the Court's language on this point leaves room for doubt as to whether its findings in relation to innocent dissemination constitute ratio decidendi or mere obiter dicta. We have to consider this in light of the High Court's finding as to the meaning of 'publication' in *Trkulja v Google LLC* [2018] HCA 25. There the High Court held (at [38] to [41]) that "all degrees of publication are publication" (at 40) and that the proper approach to pleading is for the plaintiff to simply plead publication, on the basis that the question of whether or not the defendant is a subordinate publisher only arises if the innocent dissemination defence is pleaded. So, the better view may be that the finding as to innocent dissemination is obiter.

Kevin Lynch

Eli: Marlia, can you explain the process of content moderation, and how hiding and deleting comments work? What control does a media publisher have over comments posted by third party users on Facebook?

Marlia Saunders: On public Facebook pages, there is no option to remove or disable the "Like", "Comment" or "Share" features or to pre-moderate comments before they appear. Apart from banning specific names of users (who could just pop up again with a different profile anyway), there is no way to prevent users from posting comments. Content moderation can be done by setting the "profanity filter" offered by Facebook to "strong" – Facebook will then hide any comments which contain commonly reported words and phrases marked as offensive by the community. There is also a feature on Facebook that allows a page administrator to compile a list of words which if included in a comment posted on the page will cause the comment to be hidden. This feature is generally used for profanities that may not be picked up in the automatic "profanity filter" provided by Facebook, such as uniquely Australian derogatory terms which Americans have never heard of. While I say such comments will be "hidden", a comment containing a word on these lists will actually remain visible to the user who posted it and to all of their "friends".

Otherwise, moderation must occur after a comment is posted by employing someone to manually scroll through the comments and either hide or delete them. This is challenging for a number of reasons – comments can be posted at any time of the day or night; comments can be posted in response to other comments which creates sub-threads and makes it difficult to keep track of what is new; problematic comments can be posted on even the most anodyne stories; and the volume of comments on media pages can number thousands or tens of thousands each day, and most media organisations have multiple pages dedicated to each masthead or program, which makes moderation a very time consuming and costly exercise. To give you some figures, at the hearing, evidence was given that there are around 50 articles a day posted on the Sydney Morning Herald page and each post can receive thousands of comments (at [40]). The Facebook page of The Australian

Marlia Saunders

posts about 20-30 stories per day and comments are made up to thousands of times per day (at [46]); and The Sky News and Bolt Report Facebook pages have around 60 to 80 posts times per day, and each post can receive as many as 1800 comments (at [54]). Due to the large volume of comments, email notifications of new comments are often switched off, otherwise social media editors would receive thousands or tens of thousands of emails each day.

Eli: Nine CEO, Hugh Marks, has argued that the responsibility should rest with social media platforms as the publishers, not with the news organisations. Robert, what about Facebook's role in all of this? What is expected of a platform in the moderation of third party comments?

Robert: That assumes you accept that both should have some primary responsibility beyond that of the poster and I would argue that neither the platform nor the Page Owner should immediately have such liability placed on them. However, it may be desirable that social media platforms provide the operators of public pages with the tools they need to be able to efficiently moderate third party comments published to the public. For example, Facebook does not provide an option for operators to totally disable comments on a public Facebook page, and the text filtering options available aren't comprehensive. Even if you manage to prepare an extensive list of words, the text filters will not capture emoji or image-based comments (such as GIFs or memes), nor, as noted in the judgment, will they capture comments that use alternative spellings or lettering (e.g. substituting an "S" for "$").

It should also be noted that, if one starts from the position that everyone is a publisher (as Justice Rothman seems to do), Facebook and other social media platforms are also at significant risk of being found liable as primary publishers of defamatory posts of which they have knowledge (e.g. through a complaints handling mechanism). On that basis, implementing additional controls for the individual operators of public Facebook pages in order to deal with defamatory content more easily is also to the platform's benefit in mitigating the risk of liability.

Eli: Justine, it seems that the judgment was guided considerably by the *Oriental Press* judgment of the Court of Final Appeal of Hong Kong. Can you take us through that judgment and explain why it was so persuasive? How does this judgment cooperate with other Australian online defamation judgments, such as *Duffy* and *Johnston v Aldridge*?

Justine: Justice Rothman found that *Oriental Press* was the most factually analogous case to *Voller*. *Oriental Press* concerned defamatory comments made in a forum on a public website. Only members of the website could comment in the forum, and there could be as many as 30,000 users online at any time with a peak of 5,000 comments made each hour. The webpage hosts employed two administrators to monitor the comments and delete objectionable content.

Oriental Press was particularly useful in that it canvassed the common law across several jurisdictions and the Hong Kong court considered and distinguished previous 'noticeboard' cases. It was relevant that in this case the webpage hosts played an active role in encouraging and facilitating forum postings; they derived income from advertisements placed on their website; and their business model benefitted from attracting as many users as possible to the forum. For these reasons, it was clear that the webpage hosts were publishers from the outset and were not mere conduits.

The test as to whether a publisher is a primary or secondary publisher as enunciated in *Oriental Press* was adopted by Justice Rothman – that is, whether, prior to publication, the publisher:

- knows or can easily acquire knowledge of the content of the article being published ("knowledge criterion"); and
- has editorial control involving the ability and opportunity to prevent publication of such content ("control criterion").

Justice Rothman found that the media defendants in *Voller* satisfied both the "knowledge criterion" (since the media defendants are notified of all new comments through Facebook's notification mechanisms) and the "control criterion" (because the media defendants in his Honour's view are able to "hide" or "block" comments prior to them being published by using a generic word filter, although as Marlia explains, the idea of control is somewhat illusory).

This reasoning is also consistent with the Australian authorities of *Duffy* and *Johnstone v Aldridge*. Although *Duffy* concerned a search engine that automatically published 'snippets' of website content, that judgment showed that the greater the capacity to control content in advance of publication, the more

likely it is that the disseminator will be a publisher and not a mere conduit. In other words, the extent of the disseminator's participation is highly relevant. Similarly in *Voller*, Justice Rothman found that the capacity of the media defendants to vet the comments prior to publication by using filters meant that they had a requisite degree of control and knowledge.

A key argument for the defendant in *Johnstone v Aldridge* was that it would be overly burdensome to require him to monitor and remove the objectionable content from the thousands of comments left on his Facebook post. The South Australian District Court rejected that argument and found that the volume of comments could not create a 'shield' from liability. In a similar vein, the media defendants in *Voller* claimed that continual monitoring would require a disproportionate amount of resources and would be "physically impossible" – however, Justice Rothman found that the media defendants ought to assume the risk associated with their Facebook pages, particularly when they had created them for their own commercial purposes.

Eli: How does this legal position compare to those in other jurisdictions, such as New Zealand and the UK?

Robert: As noted in *Voller*, the position in New Zealand is set out in *Murray v Wishart* [2014] 3 NZLR 722.

In *Murray*, the defendant created a Facebook page to attempt to encourage people to boycott the publication of a book about the death of infant twins and the case which acquitted their father of their murder. The book had been written by the plaintiff together with the mother of the twins, and purported to tell the mother's side of the story. The Facebook page attracted negative comments about the plaintiff, and the plaintiff sued for defamation.

A similar question arose to that in *Voller*: was the defendant the publisher of the third party comments on his page?

The court took the opposite position to that in *Voller* and held that the defendant was not the publisher. It was held that the operator of a page would only be liable for defamatory material if it knew about the defamatory material and did not remove it in a reasonable period of time (an actual knowledge test). By failing to remove it, it could be inferred that the operator of the page accepted responsibility for the third party material.

Sophie Dawson

Similarly to Justice Rothman, the NZ court also considered *Byrne v Deane*, *Urbanchich* and *Oriental Press* in making their decision.

The court rejected the "ought to know" test, finding that a person's knowledge that their page may attract defamatory material is not sufficient to found liability. The court considered the need to protect free speech, as enshrined in the *New Zealand Bill of Rights Act 1990*, and found that the "ought to know" test gives undue preference to reputation over freedom of expression. The court considered the "ought to know" test was too uncertain, and placed those that didn't know in a worse position than those who do know what is on their page (as those who do know have the opportunity to fix it).

Interestingly the court noted how difficult it would be for one person to review all comments on a popular page, and factored this into their decision.

Some significance has been attached in distinguishing *Murray* from *Voller* to the fact that Murray was operating a "private" Facebook page, and therefore did not have the same editorial controls available that the operator of a public page would have. Mr Murray gave evidence to say that he only had the following controls available:

> It is correct, however, that a creator of a Facebook page has some control over comments published on the page as he/she can, once aware of comments published, retrospectively remove individual comments and block specific Facebook users to prevent them from publishing further comments.

If Mr Murray had had the more extensive controls available to the operator of a public page, the decision may have been different. In its judgment, the court noted that it is a very fact-specific area.

No similar cases have considered the issue in New Zealand since *Murray*.

It is possible that *Voller* could impact the common law position in New Zealand, as Australia and New Zealand do consider the precedents set by the other in some cases.

In the UK, at common law, the position was that a website operator would not be liable for defamatory statements made by third parties on their website, provided that the website operator took them down when notified of them (*Tamiz v Google Inc* [2013] EWCA Civ 68).

This position changed in 2014 with the enactment of the *Defamation Act 2013* (UK). Section 5 of that Act specifically addresses the issue of the liability of website operators for defamatory material that is published on their website by a third party.

The rule under section 5 boils down to the following:

- If the author of the comment is identifiable by the plaintiff, the website owner is not liable for the defamatory material.
- If the author of the comment is not identifiable by the plaintiff, the website owner will be liable if the plaintiff gave the website owner a notice of complaint, and the website owner fails to respond within a reasonable time.

The website operator will not have a defence if the claimant demonstrates that the website operator acted with malice in relation to the defamatory material.

The fact that the website operator moderates the material published on it by others does not defeat the defence.

Liability for operators of public Facebook pages in the UK will therefore depend on whether the author of the defamatory material is identifiable, and, if the author is not identifiable, whether the operator took action upon being notified of the plaintiff's complaint.

This UK provision could potentially act as a model for reform of the Uniform Defamation Laws.

Eli: Kevin, a distinction is made between the service that a Facebook "host" provides and that which others do, including the Google search engine, and a website host. What is that distinction, and do you think that the distinction is such that it should so affect the legal position of a Facebook host?

Kevin: The distinction turned on the finding that comments on a public Facebook page can be hidden and reviewed, via the profanity filter "hack" that Marlia has described.

On the other hand, the Court said that it would be impossible, "in any meaningful way", to attribute to Google advanced knowledge of the contents of the "inordinate" number of articles which could be the subject of search published on the internet.

So that is where this Court has drawn the line. But that demarcation was in the face of evidence that the profanity filter itself is a clunky, resource-hungry and flawed mechanism to deal with the flow of third party comments posted on the defendants' Facebook pages each day.

There was an opportunity to put the defendants in this case in the same position as search engines – with notification setting up a requirement to review, consider and take down defamatory material within a reasonable time. It's not perfect, but it does set up a workable, balanced regime. Instead, commercial media organisations – and potentially others who administer Facebook pages – have been set apart.

Eli: What difference does it make that the defendants here were news organisations? Would this analysis apply equally to holding another business liable as a publisher for third party comments on a post? Should an organisation that is not a news organisation reconsider its content moderation practices, following this judgment?

Justine: Not a great deal turns on the fact that the defendants were news organisations. What is significant, however, are the findings that the media defendants had created their Facebook pages and encouraged users to comment in order to optimise readership of their news platforms and to maximise advertising revenue.

This means that any business or organisation that operates a Facebook page for commercial benefit may be liable for third party comments and will need to assess the risk of their posts attracting defamatory comments. Voller makes it clear that it is no excuse to claim that a business has insufficient resources to monitor comments; instead the Court expects that these costs will simply need to be factored into the expense of running a Facebook page.

Eli: The Court considered liability in the context of public pages hosted for commercial purposes. Do you think that non-commercial hosts – for example, NFPs, community discussion groups, government bodies, and so on – have anything to be concerned about following this judgment?

Robert: Yes. Everyone that operates a public Facebook page is in the firing line. The fact that the Facebook page may have been set up and is operating for non-commercial purposes (e.g. a charity or community discussion board) is immaterial to the question of publisher liability. Justice Rothman based the reasoning for his finding of liability primarily around the issue of editorial control of the pages, rather than the commerciality of the pages.

The operators of non-commercial public Facebook pages should also be taking steps to implement filters and monitor comments on their pages, particularly where issues discussed on their pages or posts are likely to generate defamatory comments.

Eli: Do you consider the implications of this judgment to extend beyond defamation? For example, if a media company posted a link to its article reporting on, say, a foreign conflict on which third-party users posted racist hate speech, could that give rise to liability for a media company?

Sophie: The case could well be influential in other, non-defamation, cases in which the question of responsibility for publication is raised. Section 18C of the *Racial Discrimination Act* prohibits non-private acts which are likely to offend, insult, humiliate or intimidate another person or a group of people which is done because of the race, colour or national or ethnic origin of the other person or of some or all of the people in the group. Defamation case law has been taken into account in previous cases concerning the application of section 18C, particularly in relation to the question of meanings conveyed: see *Eatcock v Bolt* (2011) 197 FCR 261 at [19], *Jones v Scully* (2002) 120 FCR

243 at [125]-[126] per Hely J; and *Jones v Toben* (2002) 71 ALD 629 at [87] per Branson J.

In relation to each statutory restriction on publication to determine responsibility for publication, it is necessary to consider the particular offence, and the mens rea for that offence. Publication offences are usually strict liability, but it is still necessary for the prosecution to establish beyond reasonable doubt that the factual elements (which usually include 'publication' or similar) of the offence are established. Criminal codes often provide for a defence of honest and reasonable mistake of fact.

In Doe v Fairfax Media Publications Pty Ltd [2018] NSWSC 1996 at [162], Fullerton J confirmed that the offence in section 578A of the *Crimes Act 1900* (NSW), which is in relation to identification of a complainant in prescribed sexual offence proceedings, is a strict liability offence and that a defence of honest and reasonable mistake is available "to a publisher who publishes material that does not identify the complainant, but which is found by objective analysis to have been likely to lead to his or her identification." Fullerton J noted that "that construction would achieve the same policy outcomes as a construction where mens rea is a requisite element of the offence.

Eli: Marlia, how should a news organisation change its content moderation practices, following this judgment, if at all? It doesn't seem like your organisation, or many others, have disabled comments on Facebook.

Marlia: The decision places news organisations in an impossible position, having to weigh up the potential legal risk of being sued over the comments of an unknown third party against the commercial benefits of maintaining a Facebook presence, which include to disseminate news content, to build brand loyalty and to drive users to news websites. Mumbrella announced in July that it had decided to stop posting links to its articles on Facebook, but I am not aware of any other news organisations which have left the platform. Businesses that want to maintain their Facebook presence could reduce their exposure by not posting links to content which could be controversial or which relate to criminal charges or court proceedings; by adding words to the filter so that comments which contain potential "problem words" are hidden; and by increasing human moderation after comments have been posted.

Justine Munsie

Eli: Would the Court's reasoning apply equally to other social media platforms, such as YouTube, Twitter and Instagram?

Justine: Much of *Voller* turned on the evidence about the mechanics and operation of the Facebook platform. For instance, notwithstanding that the media defendants argued it would be physically impossible to monitor the comments which were published at any time of the day or night, and in great volumes, the Court determined that it was possible to 'hide' the comments prior to publication by using a generic filter to capture all comments. The page owner would then be notified of the new comment, and from there, the comment could be vetted and then 'released' to the public page if deemed appropriate. The availability of this mechanism was central to the Court's finding that the media defendants had sufficient control and knowledge of the comments.

If other social media platforms offer a similar pre-publication filtering mechanism, then the Court's reasoning could also apply to comments arising from posts made on those sites as well. The question which must be asked is whether the page owner has sufficient control and knowledge of the comments being made on their post.

Eli: Let's talk freedom of speech. The judgment seemed unperturbed about any implications it might have on free speech, noting that commenters could still comment on their own individual Facebook page to their heart's content (as opposed to commenting on the post). I've seen some pretty conservative advice about risk of liability following the judgment. What is the consequence of hosts having the responsibility of moderating copious amounts of live content that may be defamatory - especially when it is difficult to test immediately whether a defamatory post is defensible?

Kevin: If you put aside the factual question as to the viability of the profanity-filter hack, his Honour's decision can be seen as an application of orthodox defamation law principles. His Honour cited *Thompson v Australian Capital Television* [1996] HCA 38 where a regional broadcaster was found to be a primary publisher, not because it participated in the production of a libel, but because it broadcast it in circumstances where it had control and supervision of the material, irrespective of time constraints.

But the case law, with its Drummoyne bus shelters and Mr Pottle's newsagency, can always benefit from some up to date thinking.

The process that is envisaged in this judgment involves a media company employing competent moderators to slave away over a hot profanity filter, conducting a front-end review and decision on hundreds of comments before they appear on Facebook. No one would see this as advancing freedom of expression.

The law has long enshrined the need for defamation law to strike a balance between "society's interest in freedom of speech and the free exchange of information and ideas" and the "maintenance of a person's reputation": *Dow Jones & Co Inc v Gutnick* (2002) CLR 575. Commercial publishers are well used to judicial criticism of their commercial imperative. This judgment suggests that the weight attached to freedom of speech and the exchange of ideas was lightened very considerably by a finding that the defendants' public Facebook pages are primarily "about their own commercial interests" [207-209].

Eli: Are these issues likely to be addressed in the course of the current review currently being undertaken?

Robert: The legal questions raised by the case are more fundamental than may be dealt with in the course of the current review, and it may be that only the High Court can resolve the issues and conflicting case law. One of the major issues both for the Courts and the review is that they don't have access to or at least a deep understanding of how the technology works and its constraints. I suspect for that reason it won't be addressed, although some of the issues have been raised and solutions proffered.

In any event, the decision is likely to fuel the rise of so called 'backyard' defamation litigation based upon defamatory social media posts. The introduction of a threshold test of harm, a proportionality test and/or the expansion of the defence of triviality (as contemplated in the review) is likely to become a practical solution, particularly when in many cases it will be difficult for a plaintiff to prove that a single Facebook comment among many thousands that may be uploaded to a social media post (such as those the subject of *Voller*) has even been seen by another person, let alone establish that the Plaintiff's reputation suffered damage as a result of the publication of that single comment.

In New South Wales, a defamation claim which is viewed as trivial can be dismissed early in proceedings as an abuse of process based on the proportionality principle, balancing the cost of the proceedings and the vindication of the plaintiff: *Bleyer v Google Inc* (2014) 88 NSWLR 670. A threshold of seriousness has also been considered to be an element of the tort of defamation in the Supreme Court of NSW: *Kostov v Nationwide News Pty Ltd* [2018] NSWSC 858. Recognising and clarifying these findings in legislation through the review would go some way towards protecting free speech.

Currently the triviality defence is difficult, if not impossible, to establish for publications on the internet. It needs to be recognised that just because something is posted on the internet, where it is technically available for anyone and everyone to view, does not mean that a large number of people will in fact see it. For example, in a post with 300 comments most viewers of the post will only view the "top" or most recent five to 10 comments. On some occasions a comment will only be highlighted to the commenter's friend or follower group - which is akin to having published the defamatory material at a small private party, rather than as skywriting for the world to see. The defence of triviality should therefore be updated to assist in stemming the tide of litigation arising from social media stoushes.

Eli: What issues are we looking to have resolved on appeal?

Marlia: In their appeal, the media organisations say Justice Rothman erred in holding that they were primary publishers of the third party Facebook comments. The media organisations say that the correct position is that a person is not a primary publisher unless the person controls the content of the communication or assents to the final form of the communication.

Here, the media companies were not aware of the defamatory comments prior to publication and we say they could not realistically control the content in advance. The media companies do not own or control the platform – they are users of Facebook's services to the same extent as individual users. Further, the media companies say that they did not assent to the comments after they were posted. The plaintiff's case was that the media companies are liable for publication upon the comments being posted by third parties, even before they were notified that the comments may be defamatory. It was accepted by the plaintiff that the media companies deleted the comments within a reasonable period of being notified of them. For this reason, the media companies say that his Honour also erred in deciding whether the defence of innocent dissemination was available. This issue was not one covered by the separate question.

The media organisations also say his Honour made an error of fact in finding that the media organisations were able to "hide" all comments from all people and thereby prevent all publication of comments pending review. We say that the "hack" put forward by the plaintiff's IT expert could not be comprehensive (for example, a comment containing a defamatory image would get through the filter, as would a comment which contained spelling errors) and, in any event, a "hidden" comment would still be visible to the Facebook friends of the commenter, and would therefore be capable of being published to them. The IT expert conceded that he could not say whether the "hack" would have been available at the time the comments in this case were posted.

The appeal is set down for 17 and 18 December 2019, and we'll hopefully get some more clarity on the issues raised here when we get that judgment.

EF: Thanks everyone!

The Ethics of Artificial Intelligence: Laws from Around the World

Paul Kallenbach, Vanessa Mellis, Annabelle Ritchie and Siegfried Clarke at MinterEllison give us a global view of the laws regulating artificial intelligence.

The use of artificial intelligence and machine learning (**AI**) driven solutions is becoming increasingly common in Australian businesses. By processing enormous amounts of information in a very short time, AI can minimise human intervention in decision making processes, and allow organisations to optimise their operations. The Minister for Industry, Science and Technology, Karen Andrews, has commented that "AI has the potential to provide real social, economic, and environmental benefits – boosting Australia's economic growth and making direct improvements to people's everyday lives".

But at what cost? When does AI overstep the mark and become a tool that does more harm than good? Are we adequately assessing AI against our current policies, legal systems, business due diligence practices, and methods to protect human rights?

In this article, we examine the creation of frameworks for the ethical use of AI in Australia and globally.

Australia

Following the release of the *'Artificial Intelligence: governance and leadership'* whitepaper by the Australian Human Rights Commission in January 2019, CSIRO's Data61 released a discussion paper to boost conversation about AI ethics in Australia (**Discussion Paper**). The Discussion Paper focuses on civilian (as distinct from military) applications of AI and adopts the view that the key to unlocking the potential of AI is to ensure that the public have trust in AI driven solutions.

The Discussion Paper draws upon international approaches, as well as those developed by companies such as Google and Microsoft, to propose eight core principles to guide developers, industry and government in ethically deploying AI driven systems, namely:

1. **Generate Net Benefits:** AI systems must generate benefits for people which outweigh the costs.
2. **Do No Harm:** Civilian AI systems must not be designed to harm or deceive people and should minimise negative outcomes.
3. **Regulatory and Legal Compliance:** AI systems must comply with all relevant laws, regulations and government obligations.
4. **Privacy Protection:** AI systems must ensure that private data is protected and kept confidential and prevent harmful data breaches.
5. **Fairness:** AI systems must not result in unfair discrimination against individuals, communities or groups. They must be free from training biases which may cause unfairness.
6. **Transparency and Explainability:** People must be informed when an algorithm is being used which impacts them, and they should be informed about what information the algorithm uses to make decisions.
7. **Contestability:** Where an algorithm impacts a person there must be an efficient process to challenge the use or output of the algorithm.
8. **Accountability:** People and organisations responsible for the creation and implementation of AI algorithms should be identifiable and accountable for the impacts of that algorithm, even if the impacts are unintended.

In addition to these eight core principles, the Discussion Paper proposes a toolkit to assist stakeholders in applying those principles. We discuss this in more detail, elsewhere in this edition of CLB, in the article *Beyond Asimov's Three Laws: A new ethical framework for AI developers.*

Developments in Europe

The EU has established a High-Level Expert Group comprised of 52 experts on AI, including representatives from academia, civil society and industry, selected by the European Commission. The group recently published its *Ethics Guidelines for Trustworthy AI* (**EU Guidelines**), following stakeholder consultation on draft guidelines. The EU Guidelines are not binding, but offer stakeholders a set of guiding principles to follow to indicate their commitment to achieving "Trustworthy AI".

The EU Guidelines start by identifying four key ethical imperatives, which reflect the EU Charter of Fundamental Rights:

- respect for human autonomy;
- prevention of harm;
- fairness;
- explicability.

From these four ethical imperatives, the guidelines then derive seven key requirements.

Like Australia's Discussion Paper, the EU Guidelines highlight the importance of non-discrimination, promoting societal and environmental wellbeing, privacy, accountability and transparency.

However, the EU Guidelines include more of a direct focus on human rights, and human agency, as well as technical robustness and safety, where Australia's Discussion Paper focuses on regulatory and legal compliance and contestability.

Notably, although the EU guidelines are not binding, they are informed by the EU Charter of Fundamental Rights which is an instrument of EU Law that lacks an Australian counterpart. The guidelines note that the four ethical imperatives are in many respects already reflected to some extent in existing legal requirements. For example, amongst the wide-reaching provisions of the European Union's *General Data Protection Regulation*, article 22 provides that a decision with legal ramifications for a person (or which would similarly seriously affect them) cannot be based solely on automated processing or profiling, in most situations.

Other developments within the technology industry

Governments are not working in isolation on the complex ethical issues which AI presents. Silicon Valley's well known preference for self-regulation has manifested itself in AI policy focused initiatives such as the San Francisco based **Partnership on AI** which counts the tech sector›s big four amongst its members. Facebook in collaboration with the Technical University of Munich has announced **$7.5 million in funding for an independent AI ethics research centre**, while Amazon is working with CSIROs US counterpart, the National Science Foundation to fund **research into fairness in AI**.

Microsoft

Microsoft recently released ***Microsoft's Vision for AI in the Enterprise***, which outlines its approach to the use of AI. This document addresses the ethical challenges raised by AI, and states that designing trustworthy AI requires creating solutions reflecting ethical principles. Trustworthy AI, the company states, requires **"solutions that reflect ethical principles that are deeply rooted in important and timeless values."** For Microsoft this includes fairness, reliability and safety, privacy and security, inclusivity, transparency and accountability. In 2018, the tech giant established an **AI and Ethics in Engineering and Research (AETHER) committee**, to bring together senior leaders to craft internal policy and address ethics in specific issues.

Google

Google has also implemented a **set of principles governing the use of AI** and has experimented with an external AI ethics panel to offer guidance on ethical issues. The principles set out Google›s objectives in assessing AI applications, include to:

- be socially beneficial;
- avoid creating or reinforcing unfair bias;
- be built and tested for safety;
- be accountable to people;
- incorporate privacy design principles;
- uphold high standards of scientific excellence; and
- be made available for uses that accord with these principles.

Google has also published a list of AI applications which it will not pursue, including technologies that cause or are likely to cause overall harm, weapons or other technologies whose principal purpose or implementation is to cause or directly facilitate injury to people, technologies that gather or use information for surveillance violating internationally accepted norms or technologies whose purpose contravenes widely accepted principles of international law and human rights.

The rise in AI no doubt presents incredible opportunities for governments, private actors and society more widely but it is not without serious ethical risks. This has prompted responses from organisations and nations worldwide. In Australia, following the release of the Discussion Paper we expect work in this space to continue.

Diving into the Deep End: Regulating Deepfakes Online

Ted Talas and Maggie Kearney, Ashurst, take us through the legal framework regulating deepfakes.

The term deepfake refers to a piece of video content that has been digitally manipulated using artificial intelligence. This technology can be used to seamlessly combine content from different sources, for example by superimposing a person's face onto a figure in a video as if the face were a mask. A deepfake can turn a person into a virtual ventriloquist's dummy, being made to appear as though they have said or done things that they have never said or done. The term deepfake, a portmanteau of "deep learning" and "fake", comes from the username of the Reddit poster that first began posting these videos online.

The potential consequences of deepfakes are significant: political leaders can be placed in compromising (and potentially election-losing) positions or even be shown to declare war on another country; celebrities can be used to endorse products or appear nude without their consent; consumers could be subject to complex phishing scams. At the same time, deepfakes can be used for less nefarious purposes, including parody, satire and entertainment (or however you would characterise inserting Nicolas Cage into every movie ever made[1]).

While the digital manipulation of visual content (whether using Photoshop or Instagram filters) is not a new phenomenon, the seamless manipulation of this content using artificial intelligence techniques is likely to present a more fundamental challenge to how we distinguish between what is fake and what is real.

In this article, we look briefly at how three areas of Australian law – copyright, defamation and the Australian Consumer Law (**ACL**) – could be used as tools to regulate the use and spread of deepfakes online. We have not attempted to provide an exhaustive list of the legal frameworks that may apply to deepfakes and acknowledge that many more could apply, including privacy laws and laws dealing with the non-consensual sharing of intimate images.

How do deepfakes work?

At this point in time, deepfakes are generally created using a machine learning framework called a generative adversarial network (**GAN**).[2] A GAN relies on two algorithms set to compete against each other. The first algorithm generates artificial samples of whatever you are trying to fake. These samples may be based off input data (eg, a collection of images of a particular person's face) or even random noise. The second algorithm compares these against a training data set to predict whether the sample is fake (ie, has been created by the generating algorithm) or real (ie, from the training data set). This process is then repeated (potentially many millions of times) with the predictions being fed back to the generating algorithm after each repetition to teach it how to make more and more realistic fakes which can be applied frame by frame to a video.[3]

While originally confined to academic work and the darker corners of the internet, since 2018, deepfake tools have been generally available online. This allows anyone with a set of photos or a video and sufficient computing power to create a deepfake (processing the repetitions required to make a convincing fake requires a relatively fast computer).

While deepfakes rely on artificial intelligence, it is important to keep in mind that it is possible to effectively manipulate videos without the use of this technology. For example, in May 2019, a video of Nancy Pelosi was released online which had been slowed so as to make Speaker Pelosi appear drunk.[4] These kinds of videos, which sometimes referred to as "cheapfakes", may be as problematic as deepfakes (for example, the Pelosi video was re-tweeted by President Trump).

Copyright

As outlined above, deepfakes ordinarily involve or incorporate existing video or audio content. Assuming this content is original, it is likely to be protected under the *Copyright Act 1968* (Cth) and copyright in the footage or recording will generally be owned by the person that made the film or recording (or their employer).

1 The A.V. Club, *Deep learning technology is now being used to put Nic Cage in every movie* (29 January 2018) <https://www.avclub.com/deep-learning-technology-is-now-being-used-to-put-nic-c-1822514573?rev=1517249018178&utm_content=Main&utm_campaign=SF&utm_source=Twitter&utm_medium=SocialMarketing>.

2 For further background, see Skymind, *A Beginner's Guide to Generative Adversarial Networks (GANs)* <https://skymind.ai/wiki/generative-adversarial-network-gan>.

3 For a useful illustration, see Australian Broadcasting Corporation, *How hard is it to make a believable deepfake?* (28 September 2018) <https://www.abc.net.au/news/2018-09-28/fake-news-how-hard-is-it-to-make-a-deepfake-video/10313906>.

4 Australian Broadcasting Corporation, *Nancy Pelosi speech manipulated to make her appear 'drunk' does not violate Facebook rules* (24 May 2019) <https://www.abc.net.au/news/2019-05-24/nancy-pelosi-speech-altered-video-slurring-words/11148030>.

If a deepfake reproduces a substantial part of the underlying film or recording, the owner of the film or recording would conceivably have a cause of action in copyright infringement against the creator of the deepfake and any person that subsequently reproduces or communicates it (subject at least to any fair dealing exception). A copyright claim may also arise in relation to the images or recordings used as the input to create the deepfake. As a part of this, the copyright owner could approach a Court to obtain an injunction to require the removal of the deepfake together with damages or an account of profits. The copyright owner could also seek to have the content removed under the takedown systems maintained by online platforms like Facebook.

The key limitation with using copyright to regulate deepfakes is that a copyright claim does nothing to vindicate – or even recognise – the damage caused by a deepfake to the person targeted by it, ie, the individual whose face and identity are used without their consent. Indeed, the person who is the target of the deepfake (and therefore likely to suffer the most harm as a result of its dissemination) is unlikely even to have standing to bring a claim for infringement or seek an injunction on copyright grounds. This is because, in the majority of cases, the target of a deepfake will not be the owner of the copyright in the underlying film. For example, if deepfake techniques are used to transplant a person's face into a pornographic video, only the maker of the video may be able to bring an infringement claim and not the person whose face was digitally inserted into the film.

Of course, where the interests of the deepfake target and the copyright owner align, this may not be an obstacle to removal of the deepfake. In June 2019, Condé Nast, the publisher of Vogue, successfully used YouTube's takedown request process to have a deepfake of Kim Kardashian West removed from the platform. The deepfake, which was created by a group of artists to lampoon influencer culture and would probably constitute fair dealing under Australia law, was based on footage from an interview Ms Kardashian West had done for Vogue in April 2019 (in which Condé Nast would have owned the copyright).[5]

However, these cases are likely to be rare, particularly for ordinary people without Ms Kardashian West's social media following. For most people, it may be impossible to identify a person whose copyright may be infringed by a deepfake. Even if such a person did exist and was identifiable, there is no guarantee they would be willing to assist the target of a deepfake by enforcing their rights as a copyright owner.

Another limitation with relying on copyright to deal with deepfakes, or indeed any of the legal frameworks discussed in this article, is that in many circumstances the creator of a deepfake may either be anonymous or located outside the jurisdiction of an Australian court. While the target of a deepfake may still be able to bring an action against an intermediary, such as an ISP or online platform, to have the content removed, these remedies may only be available in certain circumstances. This kind of intermediary liability may also have other unintended consequences, particularly given that intermediaries may face a commercial incentive to block content following a complaint rather than assessing the legitimacy of the complaint (eg, in circumstances where the alleged "deepfake" is actually real footage) or considering the applicability of any fair dealing exception.

As a result, while the law of copyright may be a useful tool to combat deepfakes in certain circumstances (particularly if the complainant is able to rely on online platforms' existing copyright takedown systems) the limitations discussed above mean that copyright law is unlikely to be a sufficient tool to address the proliferation of deepfakes online.

Defamation

Unlike copyright, the tort of defamation is specifically concerned with vindicating a person's reputation. It is not difficult to imagine a deepfake in which an identifiable individual is put into a compromising position or a scenario which could damage their reputation. The possibilities are literally endless. In these circumstances, and assuming the resulting video is made available to a third party, the target of a deepfake may be able to bring a defamation claim against any person involved in the publication of the deepfake to redress the damage to the target's reputation.

While the law of defamation has historically focused on words, whether spoken (slander) or written (libel), and is therefore well suited to address defamatory statements made in a deepfake, the law has recognised that images too can be defamatory. Famously, in *Ettingshausen v Australian Consolidated Press Ltd* (1991) 23 NSWLR 443, the New South Wales Supreme Court held that a photograph in which Mr Ettingshausen's genitals were apparently exposed was capable of subjecting the football player to ridicule and, therefore, of being defamatory. As a result, defamation law could also be used to provide a remedy in relation to the visual aspect of deepfakes.

Defamation law has also been applied to images that have been digitally altered. For example, *Charleston v News Group Newspapers Ltd* [1995] 2 AC 65 concerned an article published in *The News of the World*. The article, under the headline "Strewth! What's Harold

5 Vice Motherboard, *The Kim Kardashian Deepfake Shows Copyright Claims Are Not the Answer* (20 June 2019) <https://www.vice.com/en_us/article/j5wngd/kim-kardashian-deepfake-mark-zuckerberg-facebook-youtube>.

up to with our Madge", included a large photograph of a man and a woman nearly naked and apparently engaging in sexual activity with the faces of actors from the television soap *Neighbours* superimposed on each body. The actors sued for defamation, including on the basis that they had been made out as willing participants in the creation of the photograph.

In this case, the House of Lords dismissed the actors' claim, holding that the publication was incapable of conveying any of the defamatory meanings pleaded. This was because any defamatory sting in the photograph was effectively neutralised by the accompanying text in the article which clarified that the photograph had been produced by the makers of a pornographic computer game without the knowledge or consent of the actors.

This is not to suggest that the mere fact that a deepfake includes a disclaimer that it is the product of digital manipulation, or even if this is apparent from the poor quality of the video, will frustrate a claim for defamation. It will all depend on the imputations pleaded. For example, Senator Sarah Hanson-Young successfully brought defamation proceedings against Zoo magazine in relation to an article featuring a plainly photo-shopped image featuring Senator Hanson-Young's face on the head of a bikini model (the imputations included that the article suggested that Senator Hanson-Young was not a serious politician).

Given this area of the law focuses on vindicating a person's reputation regardless of how they are defamed, the established principles of defamation appear to be well suited to addressing the reputational harm caused by deepfakes, particularly given that Courts in Australia have a record of applying the established principles of defamation law in new online contexts.

However, although defamation may provide a mechanism for the target of a deepfake to obtain compensation, in certain circumstances, it may be a less effective mechanism to force the removal of deepfakes. This is because Australian Courts are often reluctant to grant injunctions in defamation proceedings due to free speech concerns, particularly on an interlocutory basis. However, this reluctance may not apply in circumstances where there is no public interest in the deepfake remaining available online (eg, in the context of revenge porn).

Australian Consumer Law

Unlike other jurisdictions, the common law of Australia does not recognise an independent cause of action to protect how a person's identity, including their name and likeness, is used. In jurisdictions where these publicity rights are recognised, claims based on such rights are likely to be a useful tool to be deployed against deepfakes, at least where the deepfake is used in a commercial context.

Nevertheless, a plaintiff in Australia may be able to rely on the ACL in a similar way. By way of illustration, consider a deepfake in which a famous tennis player was made to endorse, without their knowledge, a tennis racquet made by a manufacturer other than their sponsor. Such a video would potentially contravene the provisions of the ACL, for example, sections 29(1)(g), which prohibits a person, in connection with supplying or promoting goods, making a false or misleading representation that the goods have a certain affiliation, approval or sponsorship or the general prohibition on misleading and deceptive conduct in section 18.

The ACL provides for a wide range of remedies for any contravention, including injunctions and damages. Additional orders, including pecuniary penalties, are also available in enforcement actions brought by the ACCC. In addition to the ACL, our hypothetical tennis player may also be able to rely on the tort of passing off to obtain an injunction, damages or an account of profits in relation to the deepfake.

While the ACL appears to be an ideal tool to combat deepfakes (after all, deepfakes are, by definition, misleading and deceptive), in reality, its application is limited. This is because the ACL generally only applies to commercial activity. For example, the prohibition on section 18 only applies to conduct "in trade or commerce". The ACL is therefore only likely to capture deepfakes used to promote a product or service, criticise a business so as to influence consumer behaviour or where the deepfake itself is being directly monetised (eg, through the sale of online advertisements). These laws are unlikely to apply to deepfakes used in other, and potentially more insidious, contexts, such as revenge porn or political disinformation (although other more-targeted laws may apply in those scenarios).

Conclusion

While existing legal frameworks may be appropriate to regulate deepfakes in certain circumstances, these frameworks are unlikely to be sufficient to address the fundamental challenge that deepfakes pose to society.

There is no doubt a role to play for new laws dealing with the spread of deepfakes and other disinformation online.[6] However, our view is that future legislative reform will only ever form part of an effective solution. What is required is the continuing development of effective tools to detect, identify and alert internet users of deepfakes. Poetically, many of these tools rely on the artificial intelligence that makes deepfakes possible in the first place.

6 For example, the ACCC has recently proposed the creation of an industry code to govern the handling of complaints in relation to the spread of disinformation on digital platforms (and which would capture deepfakes). See Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, June 2019) 370.

The 2019 C

The annual CAMLA Cup was held on 29 August 2019 at the Sky Phoenix in which teams from all over Sydney competed to prove their savvy and intellect. There was a fantastic turn out with well over 200 participants, including teams from the ABC, Addisons, Allens, Ashurst, Ausfilm, Baker McKenzie, Banki Haddock Fiora, Beyond, Bird & Bird, CAMLA Young Lawyers, Chris Chow Creative Lawyers, Clayton Utz, Corrs Chambers Westgarth, Foxtel, Free TV, Gilbert+Tobin, Holding Redlich, HWL Ebsworth, Marque Lawyers, MinterEllison, News Corp, Norton Rose Fulbright Optus, Sainty Law, SBS, Sony and Webb Henderson.

Notwithstanding fierce competition on all fronts, MinterEllison's formidable knowledge and unshakeable savvy were rewarded with being crowned champions of the 2019 CAMLA Cup – check out their photo below. In addition to the glory of being recognised as media, technology and communications champions, the winners were awarded with double tickets to the Belvoir Theatre. Other amazing prizes included Google home minis, Sony headphones, Gelato Messina vouchers and chocolate frogs – that's right, at the CAMLA Cup, everyone's a winner!

CAMLA Cup

Other highlights of the night included an intense, three round tie-breaker between representatives from Addisons, Clayton Utz and Gilbert+Tobin to determine the winners of the Table Quiz; and the roll call of almost every High Court and Federal Court judge in a frenzied effort to answer the "Who Am I" round.

In sum, the 2019 CAMLA Cup was a great success and much fun was had by all. Not only does the CAMLA Cup encourage participants to stay on top of the latest developments in the industry by testing their knowledge, it provides a relaxed opportunity to network and improve team relations within your organisation.

If you missed out this year, be sure to keep reading the Communications Law Bulletin for the announcement of the 2020 CAMLA Cup. Both CAMLA and non-CAMLA members are welcome to attend. Join us next year to see if Minter Ellison can maintain their reign or if they will be overthrown by another deserving contender.

CAMLA wishes to thank hosts Deb Richards and Ryan Grant, organiser Cath Hill, the CAMLA Young Lawyers volunteers and the CAMLA Board for putting together another wonderful event.

Congratulations to The BoJos team from MinterEllison on your CAMLA Cup win!

Thank you to everyone who supported CAMLA's annual trivia night. We had a ball!

And a big thanks to our MCs, **Debra Richards** and **Ryan Grant**. Debra has been our trivia night host for 15-20 years and claims this was her last one. We'll see! We thank Debra for her enormous contribution to this great CAMLA tradition.

Thanks too to all the following organisations for prize donations. The night would not be the same without your support and generosity. Thank you!

ABC | Addisons | Allens | Ashurst
Ausfilm | Baker McKenzie
Banki Haddock Fiora | Beyond
Bird & Bird | Clayton Utz
Chris Chow Creative Lawyers
Corrs Chambers Westgarth
Foxtel | Free TV | Gilbert + Tobin
Holding Redlich | HWL Ebsworth
Marque | MinterEllison | News Corp
Norton Rose Fulbright | Optus | SBS
Sony | Webb Henderson

See you next year!

Interview: Richard Ackland AM

Richard Ackland AM is a lawyer, legal publisher and journalist who has written on the law for around 45 years. He is a former host of ABC TV's Media Watch and ABC Radio National's Late Night Live and is the publisher of Justinian and the Gazette of Law and Journalism. Along with Deborah Richards and Anne Connolly, he won the 1999 Gold Walkley for exposing the cash for comment arrangements between commercial radio and the banks. He currently contributes to Guardian Australia and The Saturday Paper. Richard caught up with Patrick Tyson, CAMLA Young Lawyer and Business Affairs Coordinator & Lawyer (Acquisitions) at the ABC for a discussion about press freedom, national security and news in an increasingly digital world.

PATRICK TYSON: Several commentators have observed that since 2001 successive Australian federal parliaments have passed around 75 national security and counter-terrorism laws. This exceeds the number of comparable laws passed by other Western countries such as the UK and the USA. Did the AFP's raids on the ABC and the home of News Corp journalist Annika Smethurst surprise you or was it a development you considered inevitable? What was your initial reaction?

RICHARD ACKLAND: My initial reaction? What a clumsy move by the AFP. Two raids in rapid succession – one on a News Corp journalist and the other on the ABC at its Sydney HQ. Nothing could be more likely to inflame the entire media and set off a concerted campaign to review national security laws that adversely impact news organisations. It soon became a global story about the erosion of a free press in Australia. The attempt to extract documents from the ABC is suspended while the warrant is challenged in the Federal Court.

Was it surprising or inevitable? It's not totally surprising because police have raided news organisations over the years trying to find out how classified information got into the hands of reporters. The arsenal of legislation now gives law enforcement agencies wider and wider powers to protect state secrets and penalise their publication, so it's inescapable that at some point those powers will be used.

The media also operates in a more hostile political environment. Peter Dutton, the Home Affairs Minister, has a hardline approach to national security, declaring that journalists are not "above the law" – except, it seems, when favoured journalists publish classified information from his own agencies critical of the Medevac legislation. When the Medevac Bill was going through parliament, The Australian somehow had a story about how ASIO thought the legislation would undermine regional processing and make border protection more difficult. It was widely suspected to be a security leak from Dutton's people to a supportive newspaper.

Most of the time, the government response has nothing to do with "national security" at all. National security should be about keeping citizens and the country safe from internal and external threats and attacks. Bernard Collaery and Witness K's alleged offences, the reporting of ostensible war crimes by Australian soldiers in Afghanistan, and the story about giving the Australian Signals Directorate sweeping surveillance powers, are all public interest stories and in no way threaten the security or safety of Australia.

The landscape that encompasses national security laws, leaks, and journalism is replete with political theatre and hypocrisy. The only thing the government regards as not secret are ministerial press releases.

TYSON: There was a relatively uncommon display of solidarity between Australian news media organisations in condemning the AFP's raids. Do you think that, in a perverse way, the raids have had a demonstrably positive impact on cooperation and support between sometimes opposing and competing news media organisations?

ACKLAND: I don't think there would have been media unity had the News Corp journalist, Annika Smethurst, not had her home raided and her computer and mobile phone searched.

In all other respects, News Corp remains the avowed ideological and cultural enemy of the ABC, The Sydney Morning Herald and The Age mastheads. Yes, there is a momentary meeting of minds between News Corp, Nine and the ABC that the authorities should not be putting their hob-nailed boots inside newsrooms and snooping into journalists' electronic devices. How long that happy state of affairs lasts is problematic.

It is likely that the news organisations will be disappointed with the outcome of the reform agenda they are pushing, specifically with the way warrants are issued, the protection of public interest whistleblowers, improved access to government information under FOI laws, and a restriction on the way "Top Secret" is stamped in red ink on every piece of government paper that might usefully be in the public domain. Some of those proposals are now being reviewed by the Parliamentary Joint Committee on Intelligence and Security – the committee that waved the current spate of security laws into existence.

Can you really imagine this government, in particular, giving the media any free kicks?

It is even more troubling that journalists did not do a decent job in relentlessly flagging the dangers of the security measures governments introduced following 2001 World Trade Center attacks. In many instances, elements of the media were cheering on the introduction of laws that now pose a threat to their ability to report.

TYSON: You mentioned several reforms being discussed to better protect press freedom in Australia. There have also been calls for the enshrinement of press freedom within a "Press Freedom Act" and/or a federal Human Rights Act, as well as exemptions or defences in relevant national security legislation for reporting in the public interest. What changes to the law, if any, do you favour and why?

ACKLAND: There should be a national Human Rights Act and it should have happened ages ago. The opponents of such legislation have come up with nothing more original than a mantra that only elected politicians, not judges, should be deciding policy issues. Parliament and the executive arm are not the only decision-making elements in a liberal democracy.

A Human Rights Act would have universal application for society at large, not just to the media's interest in free speech, which must be balanced against other interests and freedoms. I don't think legislation, such as a Press Freedom Act, that would reserve specific rights for the media alone would be politically palatable. What I've heard about a proposed PFA sounds vague and motherhoody. I may be wrong about that and will probably change my mind next week.

Beyond that, there are elements of the national security laws that could be amended to mitigate the chilling effect on the media. Such as:

- Having actual judges apply more than a momentary consideration to issuing search warrants. Currently, Local Court registrars and political appointees to the AAT can make these decisions, even the Attorney-General.
- If there is to be metadata retention, there needs to be contestable warrants.
- The anti-encryption legislation needs more judicial oversight with merits reviews.
- Whistleblowers from within the Commonwealth public service are hung out to dry if they leak information to the media in the public interest. For example, the Afghan Files published by the ABC and the Witness K case. Whistleblower protection is vital to enabling disclosures in the public interest.
- Having a precise definition of "national security". It currently applies to any document with "secret" stamped on it or passed over the cabinet table. National security should specifically apply to situations that endanger the life and limb of Australians and to the nation's infrastructure. At the moment "national security" is being applied farcically where the media has exposed the government's abuse of power.

TYSON: While you harbour doubts about the Parliamentary Joint Committee on Intelligence and Security, do you think any changes to the law will be forthcoming?

ACKLAND: Maybe I›m wrong to doubt Andrew Hastie MP and his merry tribe on the Committee that has awarded elephant stamps of approval to the national security legislation we have now. These are politicians who made capital by spooking the country with endless pieces of security legislation. So many in fact, that no-one knows with any fine detail what the laws mean, how they will be applied and the penalties for which journalists are potentially liable.

The net effect is that editors play it safe, spike the contentious story that gets too close to "national security" and instead give us a half-page about how to fry mushrooms.

Having said that, I would not be surprised if a few minor recommendations for change did emerge. Hastie, for instance, has been a solid defender of the work done by The Sydney Morning Herald and The Age on the influence of China and its agents on Australian politics. To that end, he has supported the journalism, even stories from well-credentialed journalists that have been battered to pieces by judges in the Federal Court.

TYSON: If editors sometimes play it safe when stories involve "national security", following the AFP raids have you noticed or experienced greater reluctance from editors, journalists or whistleblowers to be involved in such stories due to fear of personal punishment?

ACKLAND: I think there has always been nervousness about dealing with information the government does not want you to see. Remember last year when the ABC took delivery of filing cabinets full of official documents that had been sold at a second-hand auction in Canberra. Within a matter of days and after publishing a few selected stories, the ABC obediently handed the files to ASIO. The government kicked up a fuss and the public broadcaster got frightened.

The government has succeeded in spooking the media. "National security" can mean whatever the government wants, most usually information that if published would be embarrassing. If a hot "national security" story fell into the lap of a fortunate journalist there would be hours, if not days, of editorial and legal discussion trying to work out the consequences, the extent to which the information would get on the wick of the government, the likelihood of a successful prosecution, and the

costs - monetary and emotional. The greatest caution would be applied.

The principal pieces of "national security" legislation that affect journalism are relatively new – the secrecy and espionage amendments to the *Criminal Code Act 1995* (Cth), metadata retention as a result of amendments to the *Telecommunications (Interception and Access) Act 1979* (Cth), and anti-encryption measures under the *Telecommunications (Assistance and Access) Act 2018* (Cth). These laws criminalise obtaining certain information from government employees and give the state wider access to the electronic communications of journalists, and other citizens. However, as far as I know, no arrests have been made under any of these laws in response to news reporting.

Another problem is the effect on whistleblowers, on whom the media is dependent for high-level scoops on abuses of government power. Journalists have some limited defences under the laws, but not so much for whistleblowers, who face penalties of up to 10 years' imprisonment.

Journalists even face the possibility of prosecution for "dealing" with government classified information or for receiving a letter where the recipient may be ignorant of the contents.

TYSON: The AFP raids led to a visible increase in public awareness and support for press freedom. Do you expect this to be a long-term shift in the Australian consciousness or is there a risk it will quickly fade away, particularly due to the 24/7 news cycle?

ACKLAND: Something must be happening. We even had Home Affairs Minister Peter Dutton advising the AFP to take account of the "importance of a free and open press" before deciding to raid journalists' homes and workplaces. He added: "Where consistent with operational imperatives, I expect the AFP to exhaust alternative investigative actions prior to considering whether involving a professional journalist or news media organisation is necessary."

Richard Ackland AM

Maybe Dutton was just making nice to News Corp, the favourite and compliant destination of ministerial leaks.

As for being a "long-term shift in Australian consciousness" for press freedom, we need to remember that significant sectors of the media are anything but "fair and balanced", that news is distorted and dishonest agendas are hammered daily. As a result, community trust in the media, with a few notable exceptions, is at a low ebb. Until that is repaired, I suspect most members of the community do not give a fig about press freedom.

TYSON: What effect, if any, do you think the issue of press freedom has had on Australia's reputation and influence internationally?

ACKLAND: Surprisingly significant. In this year's Reporters Sans Frontières (RSF) World Press Freedom rankings, Australia dropped two places to #21, behind Costa Rica, New Zealand, Jamaica, Uruguay and Surinam.

The concentration of Australia's mainstream media is one factor that impacts press freedom.

Then we have the most dreadful defamation regime of any comparable democracy, pathetic FOI laws, endless court suppression orders, government lockdowns on reporting on Manus and Nauru, and draconian security laws that inhibit whistleblowers and reporters. As RSF reports, Australia has news and information "black holes".

Following the raids on the ABC and Annika Smethurst, I received a call from public radio in Sweden and was asked to comment on what was going on with press freedom in this country. The Swedes were interested! There was also wide reporting in the UK, USA, Europe and throughout our region. It's troubling and embarrassing that successive Australian governments treat citizens as children, or worse, mushrooms who should be kept in the dark.

TYSON: Press freedom is one of many important issues affecting news media. Digital disruption has undeniably transformed the global media environment over the last couple of decades. How well do you think Australia's traditional news media (newspapers and broadcasters) have innovated and adapted in the new digital era? Is there an area where they are failing to connect with modern audiences?

ACKLAND: Many large and important media organisations feel they could have handled the transition better. For years stories were posted on the internet where they could be read for free. By the time management decided that paywalls were necessary to keep the show afloat, it was too late – most people had gotten used to having their daily journalism for nothing. It's been a struggle ever since to get people back behind the paywalls and it took a long time for the news publishers to go "digital-first". In any event, digital publishing is not generating enough revenue to fund operations properly.

There have been some terrific new digital entrants – Guardian Australia prime among them – with open content. The ABC news website is also a wonderful resource – no wonder the commercial publishers are squealing that the national broadcaster is eating their lunch.

The internet has atomised sources of information so people can find things of specific interest that are not part of the diet of the dailies. That will be an ongoing trend. General news accompanied by narrow silos.

I think print newspapers will survive as they become more local, with greater concentration on investigations with "star" reporters and columnists. At least I hope they survive. I can't imagine life without daily newspapers. Although, Millennials and Gen-Z already seem to survive in a print-free world.

TYSON: While you are a fan of the traditional print, are there digital tools you think have the potential to innovate news further or generate new revenue streams?

ACKLAND: I don't think there has been a truly successful news app that brings you digests of and links to stories of specific and specialised interest. Apple has a news alert but the targeting seems a bit wonky. Others have tried, but there's still a gap in the app market for something that is truly terrific that tells you everything you really want to know.

Maybe this could be developed by biometrics or identifying readers' needs by their thumbprint. Another important breakthrough could be for Google to install chips in our head whereby all the important things can be transferred into our brains without having to read or make sense of what is written.

Patrick Tyson is a CAMLA Young Lawyer and Business Affairs Coordinator & Lawyer (Acquisitions) at the ABC

CAMLA Young Lawyers

Challenges and Opportunities in the Telco Sector panel discussion

By CAMLA Young Lawyer Committee representative Amy Campbell (HWL Ebsworth)

An opposed merger. The next-generation of mobile networks rolling out. Huawei blocked. Shifting national security policies, powers and risks. The Young Lawyers' idea for the "Challenges and Opportunities in the Telco Sector" panel discussion was conceived against this backdrop.

The esteemed panellists - Cameron Cross (General Counsel, nbn), Thomas Jones (Partner, Bird & Bird), Simone Sant (Deputy General Counsel, Vodafone) and Martyn Taylor (Partner, Norton Rose Fulbright) - brought the topic to life on the evening of 14 August in front of a crowd of 76 attendees at Bird & Bird's offices.

The audience heard the leading panellists highlight the dynamic nature of the telecommunications sector, distil some of the complexity around current issues and offer their insights on developments and risks they anticipate in the short term and into the future.

The core areas discussed included:

- How 5G works, the extent to which it will be "transformational", what impact 5G is likely to have on service providers and the legal issues that may arise.
- Implications of 5G on competition for the supply of existing telco services.
- Merger trends in the telco space.
- Policy reasons for the Huawai ban set against the extensive use of Huawai equipment in Europe.
- The current regulatory landscape and anticipated reforms following the federal government's review of metadata retention laws.

The Young Lawyers Committee again expresses our gratitude to the excellent panellists for sharing their time and insight, to the engaging moderators - our very own Eva Lu (Thomson Geer) and Christian Keogh (Webb Henderson) who organised the event with Katherine Sessions (Office of the eSafety Commissioner) and Amy Campbell (HWL Ebsworth), and to Bird & Bird for its continued hospitality and generosity.

Profile: Dr Matt Collins QC

Dr Matt Collins QC is one of Australia's leading media law barristers, and author of renowned texts such as *The Law of Defamation and the Internet* and *Collins on Defamation*. He has appeared in some of Australia's most high profile media law matters, including appearing for Rebel Wilson against Bauer Media, and is currently acting for the ABC in relation to the raid on its Ultimo headquarters in June this year. Dr Collins recently spoke with CAMLA Young Lawyers representative and lawyer at Corrs Chambers Westgarth, Madeleine James, about a range of topics including privacy, contempt, and how to fix our "failing" defamation laws.

MADELEINE JAMES: Your career has seen you represent several major news organisations and networks, not to mention literally writing the book on defamation law. How did you find your way to specialising in this area? What draws you to it?

MATT COLLINS: I fell into media law by accident – a chance file that landed on my desk while a solicitor at a major law firm. I was immediately struck by the weighty issues that are always at play in media cases – the conflict between the right to reputation and freedom of expression – but also by the human element that that conflict invariably carries with it. In my experience, almost every defamation defendant believes they had an entitlement to publish. Often the plaintiff is a household name and the defendant a media organisation upon which we all rely for news. These features make defamation cases endlessly fascinating.

JAMES: You have written previously that several aspects of Australian defamation law are "crying out for legislative correction". Now that the Defamation Working Party has been convened to review the Model Defamation Provisions, what are the key areas you would like to see examined?

COLLINS: I believe our defamation laws are failing in two fundamental ways: they do not provide plaintiffs whose lives can be ruined in a heartbeat, often by posts on social media, with an efficient and cost-effective remedy; and they do not provide adequate protection for public interest journalism upon which the health of our democracy and institutions relies. I would like to see two fundamental reforms: the introduction of a cost-effective declaration of falsity remedy, independent of defamation law, enabling plaintiffs in appropriate cases to obtain quickly a curial finding that something published about them was false; and reversal of the presumption of falsity in defamation law, so as to require plaintiffs to prove the falsity of any imputation of which they complain and bring defamation law into line with comparable causes of action such as misleading and deceptive conduct and injurious falsehood.

JAMES: A point of difference among submissions received by the Defamation Working Party to date is whether to extend the right to sue for defamation to corporations. Do you think corporations should be able to sue for defamation? What impact would such a reform have on the Australian media?

COLLINS: Corporations were historically able to sue for defamation in Australia. Their rights were first curtailed in NSW in 2002, and then throughout Australia from 1 January 2006. The limitations on corporations under the current law depend principally on whether the corporation had fewer than 10 full time or equivalent employees at the time of publication. That limitation is arbitrary and unsatisfying from the perspective of the coherence of the law. It would, to my mind, make more sense to restrict the right of corporations (of whatever size) to sue to those cases where they can prove that a publication has caused serious financial loss.

JAMES: The Defamation Working Party has also indicated that they will consider a number of changes that would align Australian defamation law with UK positions, for example adopting a single publication rule, and changing our approach to qualified privilege. In your experience working in both Australia and the UK, how does Australian defamation law compare to the UK in terms of addressing the reality of modern media?

Collins: Australia's uniform defamation laws were passed in 2005 – the year after Facebook was founded, the year before Twitter was established, and two years before the first iPhone was released.

They are laws that predate the modern internet age. The *Defamation Act 2013* (UK), on the other hand, which commenced operation in 2014, introduced a range of reforms related to online publications, learning from earlier reforms in the United States and elsewhere. Australian law has been left behind, with the result that courts and practitioners here must resort to drawing inapt analogies in internet cases with postcards from the seaside, noticeboards in golf clubs and library card catalogues. The UK reforms are worthy of careful consideration.

JAMES: While you have appeared for numerous defendant media companies in defamation cases, you have also appeared for plaintiffs, notably Rebel Wilson in her suit against Bauer Media. Do you think defamation law fairly balances the interests of plaintiffs and defendants?

COLLINS: If you were starting from scratch, you would not come up with our current defamation laws, whose origins stretch back to the days of the Star Chamber, and depend upon presumptions of falsity and damage that tilt the balance in favour of the plaintiff and leave defences of uncertain application to do almost all of the heavy lifting. A modern defamation law would grapple much more directly with the interests at stake. Has the plaintiff's reputation been damaged? If so, is the public interest in freedom of expression such that, in the circumstances of the particular case, the plaintiff should be deprived a remedy?

JAMES: Your research explores the intersection of freedom of speech and a right to privacy. Does Australian law strike an appropriate balance?

COLLINS: Australian law does not recognise a cause of action for invasion of privacy of the kind that has evolved in countries such as the United States, the United Kingdom, Canada or New Zealand. This has led to distortions in Australia, because plaintiffs whose privacy has been infringed are either left without a remedy, or are forced to attempt to shoehorn their grievance into a claim for breach of confidence or defamation. International law has long recognised that individuals have a fundamental right to privacy. That Australian law does not protect that right is, I think, unsatisfactory.

JAMES: After representing the Australian news organisations and journalists accused of breaching suppression orders made concerning Cardinal George Pell's trial, I would be interested to hear your thoughts on the way suppression orders are currently used, and how effective they can be in the age of digital (and global) media.

COLLINS: The Pell matter is ongoing, so I will not comment on it. I share the widely held view, however, that the prevalence of suppression orders generally, particularly in Victoria, is problematic. I would like to see research undertaken into the extent to which the instinct that pre-trial publicity prejudices potential jurors is sound.

JAMES: Lastly – the media law community was recently abuzz regarding a decision of the Supreme Court of NSW that media organisations can be considered publishers of third-party comments on Facebook. What's your take on this?

COLLINS: Reasonable minds can differ about this question. On the one hand, media organisations choose, for their own commercial reasons, to use third party platforms that they do not control on which third parties are free to post defamatory comments, and could avoid the risk of liability by making different commercial decisions. On the other hand, requiring media organisations to retain control over and pre-moderate all third party comments would reduce diversity and stifle public discourse. I think the balance is better struck in the *Defamation Act 2013* (UK), where proceedings can only be brought against a person who is not the author, editor or commercial publisher of defamatory matter if it is not reasonably practicable to bring an action against the author, editor or commercial publisher. The UK provision presumes, in effect, that defamation proceedings should be brought against the primary publisher, who will also be the party best placed to prosecute any available defences.

Madeleine James is a CAMLA Young Lawyers representative and a lawyer at Corrs Chambers Westgarth

Beyond Asimov's Three Laws: A New Ethical Framework for AI Developers

Paul Kallenbach, Vanessa Mellis, Siegfried Clarke at MinterEllison

In 1942, science fiction author Isaac Asimov introduced the world to *The Three Laws of Robotics* in his short story *Runaround*. The simple rules to not injure, to obey and to protect have become a touchstone for science fiction authors ever since. However, regrettably for real world developers incorporating artificial intelligence and machine learning (**AI**) into their systems, these modest commands offer very little guidance on the real world ethical considerations which they face.

Given the particular breadth of applications for AI, it is also difficult to point to any single law or set of laws that are relevant for Australian AI developers. In any given project, a myriad of laws may be relevant. Depending on the project, this might include a combination of government specific legislation (e.g. the *Social Security (Administration) Act 1999*), human rights obligations, anti-discrimination legislation, data sharing legislation and the *Privacy Act 1988* (Cth), none of which has been developed with AI technologies in mind.

Acknowledging these challenges, the Australian government has recently joined jurisdictions around the world and started work on a framework to assist decision makers and developers to create and deploy AI driven technologies responsibly. While this article focuses on Australia's efforts, more information about developments abroad is discussed elsewhere in this edition of CLB in our article *The Ethics of Artificial Intelligence: laws from around the world.*

AHRC White Paper: Artificial Intelligence: governance and leadership

Following an inquiry, in January 2019 the Australian Human Rights Commission released a White Paper entitled ***'Artificial Intelligence: governance and leadership'*** which highlighted a number of key ethical concerns linked to AI:

- **Human dignity and life and apportionment of responsibility:** The effect of AI informed decision making and systems on everyday life is unprecedented and raises myriad questions regarding how we, as a society, should apportion responsibility and accountability when things go wrong.
- **Fairness and non-discrimination:** AI can be a powerful tool for identifying trends, bias and discrimination in decision making. However, using AI-informed decision making runs the risk of perpetuating existing trends, biases and discrimination. If the algorithm is trained on data that has trended towards favouring a certain demographic, gender or ethnicity, then the algorithm may continue to make decisions that follow those ingrained biases. There is currently no legal framework that implements safeguards at the design, modelling and execution phases of technological development.
- **Data, privacy and personal autonomy:** The personal data that individuals provide in return for services has become a highly valuable commodity. Private organisations hold large amounts of data containing personal information which can be analysed and on-sold to advertisers seeking new markets.

Data61 Ethics Framework

Following the White Paper, the Department of Industry, Innovation and Science published the ***Artificial Intelligence: Australia's Ethics Framework*** (**Framework**) authored by CSIRO's Data 61 to discuss how to best harness the benefits of AI technology, while limiting the risks which accompany it.

Given the pace and breadth of development in AI, government, industry and developers will each need to play their role in addressing ethics. The Framework is intended to create a dialogue and serve as a starting point to help guide decision making and to engender trust.

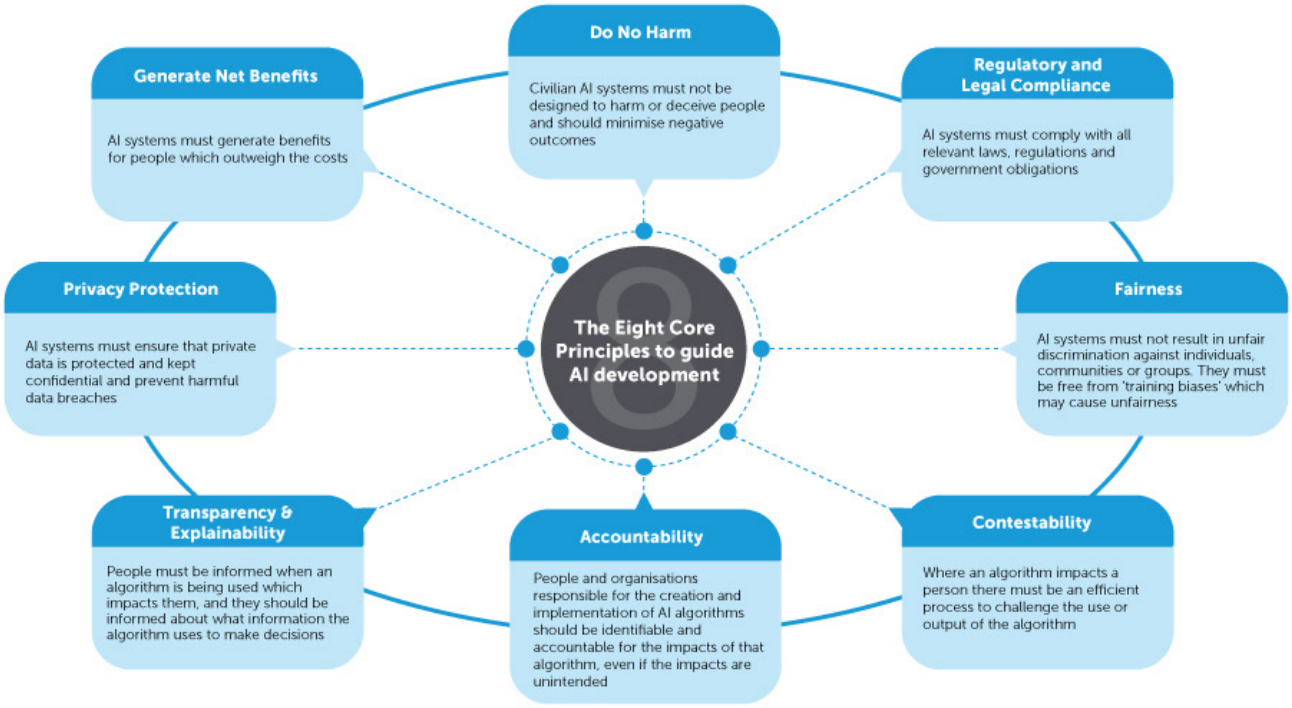
In developing the Framework, CSIRO's Data 61 formed the view that to truly unlock the potential of AI the public will need to have trust in AI applications. One mechanism to achieve this is aligning AI application development with ethical and inclusive values from the outset. It is not about rewriting laws or ethical standards but updating them so they can be applied in the context of new AI technologies.

The Framework draws on a number of complementary works and case studies from around the world to identify eight core principles which it suggests should guide AI development. See facing page:

The Ethical Development Toolkit

In addition to the eight core principles the Framework also proposes a 'toolkit' to help individuals, teams and organisations practically apply these core principles to their work. The Framework emphasises that there is no 'one-size fits all' solution when it comes to addressing ethics in AI, and it notes that the issues are challenging and not likely to remain static over time. As a starting point it extols those responsible for AI systems to ask

- what is the purpose of this system?
- which principles will guide the ethical use and deployment of the system?; and



- how would the requirements of meeting those principles be assessed?
- The Framework suggests a number of tools which might go to assist stakeholders in understanding how their systems express and incorporate these core principles. The tools include:
- **Impact assessments:** auditable assessments of potential direct and indirect impact of AI which address the potential negative impacts on individuals, communities and groups and mitigation procedures.
- **Internal or external review:** undertaken either by specialist professionals, groups or even in some cases other software to report on how the system is operating and whether it is adhering to ethical principles and applicable laws.
- **Risk assessments:** in particular with respect to assessing as a threshold matter whether certain uses of AI require additional assessment or review.
- **Best practice guidelines:** in particular to provide a flexible, accessible cross-industry guide for developers to implement that is adjusted as both technology and experience develop over time.
- **Industry standards:** in particular in the form of certification or standards which can be used as a short hand to assess off-the-shelf solutions. At this stage there is no agreed standard for AI systems or data science generally; however, both Standards Australia and the International Standards Organisation are working to develop technical and ethical standards in this space.
- **Collaboration:** programs that incentivise ‹ethical by design› AI drawing together industry and academia and groups from different backgrounds, combatting demographic bias and ensuring robust parallel development of ethical standards and technology both in theory and practice.
- **Monitoring and improvement mechanisms** which regularly review the outcomes of the system for accuracy, fairness and suitability – including whether the original goals of the algorithm remain relevant.
- **Recourse mechanisms** to create a path for appeals and human review of potentially erroneous automated decisions.
- **Consultation:** public or specialist consultation to provide an opportunity for ethical issues to be discussed by key stakeholders, including (as relevant) academics, industry and the public. In particular, the Framework notes the value of consultation in understanding the full breadth of ideas, concerns and solutions regarding ethical development of AI systems.

As developments in AI advance, governments and private actors seem acutely aware of the serious ethical considerations at play but are loath to miss out on the opportunities which AI technology presents. It is unlikely that anything as elegant as Asimov's Three Laws will ever be feasible as a rule of law; however, legislation will no doubt evolve to keep pace as the sector consolidates. With the community consultation window for the Framework having closed on 31 May, and the return of the incumbent government, we can expect developments in this space to be ongoing. In the meantime, governments abroad and major players in the tech sector are forming their own frameworks and best practices to address the ethical risks which advancements in AI pose.

Electronic
COMMUNICATIONS LAW BULLETIN

CAMLA is pleased to offer our members the Communications Law Bulletin in electronic format.

Please contact Cath Hill: contact@camla.org.au or (02) 4294 8059 to indicate your delivery preference from the following options if you have not done so already:

☐ Email ☐ Hardcopy ☐ Both email & hardcopy

The CAMLA Board for 2019

President: Martyn Taylor
(Norton Rose Fulbright)

Vice President: Gillian Clyde
(Beyond International)

Vice President: Debra Richards (Netflix)

Treasurer: Katherine Giles (MinterEllison)

Secretary: Rebecca Dunn (Gilbert + Tobin)

Julie Cheeseman (Ashurst)

Chris Chow (Chris Chow Creative Lawyers)

Sophie Dawson (Bird & Bird)

Jennifer Dean (Corrs Chambers Westgarth)

Ashleigh Fehrenbach (MinterEllison)

Eli Fisher (Baker McKenzie)

Ryan Grant (Baker McKenzie)

Emma Johnsen (Marque Lawyers)

Rebecca Lindhout (HWL Ebsworth)

Marlia Saunders (News Corp)

Raeshell Staltare-Tang (Bird & Bird)

Tim Webb (Clayton Utz)

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

BOOST YOUR CAMLA
CORPORATE MEMBERSHIP

Why limit your CAMLA corporate membership to just 5 members?

Add your colleagues for only $60 per person per year so they too receive the many benefits of CAMLA membership including an annual subscription to the *Communications Law Bulletin* and discounts on CAMLA seminars.

if you'd like to take advantage of this great offer, Please contact Cath Hill at:

contact@camla.org.au

Bird & Bird & CAMLA Invitation

Open Justice Seminar: now & in the future

16 October 2019 @ 5.00 pm

Bird & Bird
Level 22, MLC Centre
19 Martin Place
Sydney NSW 2000
Click for directions

We invite you to attend our seminar on **Wednesday, 16 October at 5 pm** to explore and discuss Open Justice. Open Justice is an essential feature of our judicial system, and has never been more topical.

This seminar will provide an opportunity to hear directly from **The Honourable T.F. Bathurst AC, Chief Justice of New South Wales** about this important principle. The Bird & Bird media team will provide an update on key principles and review processes.

Kiah Officer (Nine Entertainment Co) and **Gina McWilliams** (News Limited) will also give their perspectives as senior in-house media lawyers.

If you are interested in attending this seminar please register by **Wednesday, 9 October 2019 at www.camla.or.au/seminars** - CAMLA members $70 (incl GST); Non-members $95 (incl GST).

Program

Keynote: The important role of open justice in our system	*The Honourable **T.F. Bathurst AC**, Chief Justice of New South Wales*
The UK Perspective	***Phil Sherrell**, Partner, Bird & Bird, London*
Open justice fundamentals An overview of key case law, legislation and current review processes	***Bird & Bird media team**, Australia*
Panel Discussion: The daily battle to keep our courts open: Open justice in practice. Access to information about cases, and opposing suppression orders. What works in practice? What practical measures can be taken to increase access to information about what happens in Courts, particularly in rural areas?	***Kiah Officer**, Nine Entertainment and **Gina McWilliams**, News Limited*

Key contacts

Sophie Dawson, Partner
Jarrad Parker, Senior Associate
Raeshell Staltare, Senior Associate
Joel Parsons, Senior Associate

twobirds.com

Abu Dhabi & Amsterdam & Beijing & Berlin & Bratislava & Brussels & Budapest & Copenhagen & Dubai & Dusseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Luxembourg & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & San Francisco & Shanghai & Singapore & Stockholm & Sydney & Warsaw

1269973.1

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)