CAMLA COMMUNICATIONS LAW
BULLETIN
Communications & Media Law Association Incorporated
Volume 38, No 2. June 2019

# The Concerns and Competing Interests Surrounding Australia's New Social Media Legislation

**Sophie Dawson[1], Partner at Bird + Bird, considers the changes to the Criminal Code following the Sharing of Abhorrent Violent Material amendment in April this year.**

### Key takeouts:

Internet content services and hosts should:

- review their take down procedures to ensure they are consistent with the new law;
- ensure that their staff are trained in relation to compliance with the new law;
- consider in advance their position in relation to various likely types of content that could trigger this law; and
- ensure that their procedures take into account other media and internet laws, including statutory restrictions on publication.

## Introduction

Australia's internet and media laws have just become even more complex. A further element of complexity was added with the passage of, and assent to, the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (**Act**). The Act was passed through both Houses of Parliament on Thursday, 4 April 2019, and given royal assent on Friday, 5 April 2019. This law comes as a response to the horrific, 17-minute-long livestream of the Christchurch massacre on Facebook on 15 March 2019, which was widely shared across a myriad of online platforms.

## Existing regulatory landscape

Australia already has a large number of publication laws. Many of them are under state and territory legislation. Clause 91 of Schedule 5 of the *Broadcasting Services Act 1992* (Cth) protects internet service providers and internet content hosts from liability under state and territory laws until the host or ISP is aware of the "nature of" the content in question.

There are also relevant offences already in the Commonwealth Criminal Code. For example, section 474.17 makes it an offence to use a carriage service in a way that reasonable persons would consider to be menacing, harassing

1 With thanks to Hamish Fraser and Rohit Dighe for their contributions to an earlier version of this article.

## Contents



CAMLA

**Editors**
Ashleigh Fehrenbach and Eli Fisher

**Editorial Assistant**
Imogen Yates

**Design | Printing | Distribution**
MKR Productions

# Editors' Note

In amongst EOFY parties, AFP raids and end of season sales, June also brings to you the mid-year edition of the CLB for 2019.

Much has happened since our April publication, including the recent **Australian Federal Police raids** of the ABC's headquarters in Sydney which caused quite a stir. The raids resulted in wildly divergent views and we have canvassed some of those from high-profile commentators inside, with many thanks to **Marlia Saunders**. On the subject of media rights, CAMLA Young Lawyer representative **Antonia Rosen**, from Bankis, interviews **Larina Alick**, at Nine, on the future of suppression orders and our friends at **Ashurst** get us up to speed on defamation law reform and the recent amendments to s115A of the Copyright Act. Bird and Bird's **Sophie Dawson** provides an insight into the world of violent and abhorrent material and HWL's **Rebecca Lindhout** and **Andrew Miers** look at the recent statistics from the OAIC on data breaches. **Eli Fisher** chats with **Anna Johnston**, privacy guru at Salinger, about all things data. And **Dr Mitchell Landrigan** gives us his thoughts about the Folau/ARU stoush. Despite revving up over Redbubble's use of its copyright, Hells Angels were met with nominal recourse by the Federal Court as discussed by HWL's **Laksha Prasad**.

Further to these developments, both **Jetstar** and **Sony** have felt the early sting of the **ACCC**, both for allegedly making false or misleading representations to consumers on their respective websites regarding refunds and in Sony's case, replacement or repairs for faulty games. In the world of privacy, **ANU**, **Westpac** and the **Australian Catholic University** have become embroiled in data breach territory.

Following on from our December 2019 edition, **Geoffrey Rush** has been awarded $2.9million in his defamation case against The Daily Telegraph. It is the largest ever defamation payout to a single person in Australia after the Victorian court of appeal last year significantly dropped the actor **Rebel Wilson's** damages over defamatory articles in Woman's Day magazine. Before you ask, yes, there has been an **appeal** which will be heard August this year. Stay tuned!

In amongst all this action, the CAMLA **Young Lawyers** committee held their annual **networking event** at **MinterEllison**, where the winners of the CAMLA **essay competition** were also announced. CAMLA Young Lawyer representative **Madeleine James** provides her report on the sold-out event. Lastly, save the date - 29 August 2019 - for this year's **CAMLA Cup**. Tickets are now on sale for everyone's favourite trivia night!

For more, read on.

**Eli and Ashleigh**

***Correction**: We would like to acknowledge Jess Millner and her article "Stranger Than Fiction: The Truth Behind 'Fake News.'" The author's details were omitted in our April 2019 edition.

or offensive. Section 474.22 makes it an offence to access, publish or transmit child abuse material. And section 474.25 makes it an offence for an internet content provider or internet content host to fail to report child pornography material to the Australian Federal Police within a reasonable time after becoming aware of it.

## What does the Act apply to?

The Act contains offences which apply to internet service providers, content services and hosting services in relation to a failure to remove or report 'abhorrent violent material'.

Material will only be "Abhorrent violent material" if it meets four criteria. First, the material must be in the nature of streamed or recorded audio, visual or audio-visual material.

Second, it must record or stream "Abhorrent Violent Conduct" which is defined to include terrorist acts, murder, attempts to murder, torture, rape and kidnap.

Third, it must be material which reasonable people would regard in all the circumstances as being offensive. As further discussed below, this element of the offence may be construed restrictively in light of the High Court decision in *Monis.*

Fourthly, it must be "produced" by a person (or 2 or more persons) who engaged in, conspired to engage in, attempted to engage in, or aided, abetted, counselled or procured, or who was knowingly concerned in the Abhorrent Violent Conduct. It does not therefore apply in respect of material prepared by journalists (though it may apply in respect of any streaming by a journalist of footage originally produced by a perpetrator of the relevant conduct).

## Failure to report

Section 474.33 makes it an offence for an internet service provider, content service or hosting service (together, the **Regulated Providers**) to fail to refer material to the Australian Federal Police where the relevant person:

- is aware that the service provided by the person can be used to access particular material that the person has reasonable ground to believe is abhorrent violent material that records or streams abhorrent violent conduct that has occurred, or is occurring, in Australia; and
- does not refer details of the material to the Australian Federal Police within a reasonable time after becoming aware of the existence of the material.

It is important to bear in mind that this is not the only offence relating to failure to report crime. For example, under section 316(1) of the *Crimes Act 1900* (NSW), it is a crime punishable by up to 2 years in prison to fail to report a serious indictable offence.

## Failure to remove

Section 474.34 makes it an offence for a person to fail to ensure the expeditious removal of abhorrent violent material from a content service provided by that person.

The fault element in relation to such material being accessible through the service and in relation to failure to expeditiously remove it is recklessness.

This underlines the importance of ensuring that appropriate training and compliance procedures are in place.

Defences to this offence are expressly provided for in section 474.37(1) which provides that the offence in 474.34(1) does not apply where:

- the material relates to a news report, or a current affairs report that is in the public interest and is by a person working in a professional capacity as a journalist;
- the accessibility of the material relates to the development, performance, exhibition or distribution, in good faith, of an artistic work;
- the accessibility of the material is for the purpose of advocating the lawful procurement of a change to any matter established by law, policy or practice in an Australian or foreign jurisdiction and the accessibility of the material is reasonable in the circumstances for that purpose;
- the accessibility of the material is necessary for law enforcement purposes, or for monitoring compliance with, or investigating a contravention of a law;
- the accessibility of the material is for a court proceeding;
- the accessibility of the material is necessary and reasonable for scientific, medical, academic or historical research; or
- the accessibility of the material is in connection with and reasonable for the purpose of an individual assisting a public official in relation to the public official's duties or functions.

## Constitutional considerations likely to affect construction of the Act

When construing the Act, Courts are likely to take into account the implied freedom of speech in relation to government and political matters.

The Act expressly provides that it does not apply to the extent that it would otherwise infringe the implied constitutional freedom of speech, and refers to section 15A of the *Acts Interpretation Act* which provides that "Every Act shall be read and construed subject to the Constitution, and so as not to exceed the legislative power of the Commonwealth, to the intent that where any enactment thereof would, but for this section, have been construed as being in excess of that power, it shall nevertheless be a valid enactment to the extent to which it is not in excess of that power."

The test for whether a law is compatible with the implied constitutional freedom is as follows (see *McCloy v New South Wales* [2015] HCA 4):

1. Does the law effectively burden the freedom in its terms, operation or effect?
2. If "yes" to question 1, are the purpose of the law and the means adopted to achieve that purpose legitimate, in the sense that they are compatible with the maintenance of the constitutionally prescribed system of representative government?
3. If "yes" to 2, is the law reasonably appropriate and adapted to advance that legitimate object?

The High Court decision in *Monis v The Queen*[2] provides guidance to the approach likely to be taken by courts to the new offences contained in the Act. In that case, the High Court had to consider the meaning of 'offensive' in section 471.12 of the *Commonwealth Criminal Code*, which makes it an offence to use the postal service in a way that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive.

The High Court in that case found that the law in question did burden the freedom, such that the answer to the first part of the test above was "yes". There can be little doubt the same will be true in relation to the new offences.

The High Court also found that it had to construe "offensive" in 471.12 narrowly in order to ensure that the offence was compatible with the constitutional freedom. The communications sent by Mr Monis in that case were found not to be sufficiently offensive to meet the high bar set by that test.[3]

## eSafety Commissioner Notices

The eSafety Commissioner can issue notices which have the effect of shifting the onus of proof in relation to the element of recklessness to the accused in certain circumstances where the material remains up at the time the notice is issued. There is a presumption of recklessness unless the person adduces or points to evidence that suggests a reasonable possibility that, at the time the notice was issued, the person was not reckless as to whether the specified material was abhorrent violent material.

## Penalties

The criminal penalties under the law are significant. Failure to notify has a maximum penalty of 800 penalty units. Commonwealth Penalty units are currently $210, making the total penalty up to $168,000 for each offence.

The offence of failing to expeditiously remove or cease to host abhorrent violent material attracts a fine for a body corporate of not more than the greater of 50,000 penalty units (currently $10,500,000) or 10% of the annual turnover of the body corporate. For the same offence, an individual who is a content service provider or hosting service provider is punishable by imprisonment for a period of not more than 3 years or a fine of not more than 10,000 penalty units ($2,100,000) or both.

2 [2013] HCA 4

3 Media and Internet Law and Practice, Thomson Reuters, 1A.100

# **Interview:** Larina Alick

**CAMLA Young Lawyers representative and lawyer at Banki Haddock Fiora, Antonia Rosen, catches up with Larina Alick, Editorial Counsel at Nine Publishing and Australian Community Media, for a chat about defamation reform and suppression orders - the age old issues and the heralds of change.**

**ANTONIA ROSEN:** 2019 feels like an exciting time to be a media lawyer. There have been murmurs of change, particularly with the defamation law reform. Do you have hope that change is coming?

**LARINA ALICK:** I think change has to happen. The fact that this process has begun has surprised even me. We hoped for it, but I don't think anyone really thought it would happen because we've been waiting for it for so very long – and yet here we are! So I think there will be changes. I hope that a lot of them will be in favour of freedom of expression, which of course means in favour of the media just by the nature of the beast. The way the Defamation Act has been interpreted for the past 14 years is distinctly in favour of the plaintiff. There has been a real sense that the media are being held to a standard that no one could possibly meet particularly with qualified privilege, but also when it comes to truth. The justification defence refers to "substantial truth", but that adjective has been pretty much thrown out the window. We've been held to a standard of proof which is almost impossible for any publisher to meet, particularly when you're talking about personal circumstances and personal conduct that only the plaintiff knows about.

**ROSEN:** It's interesting that the objectives of the *Defamation Act 2005* in New South Wales and the terms of reference refer to freedom of expression and discussion of matters of public interest and importance. Do you think we've lost sight of those objectives?

**ALICK:** Absolutely. I haven't looked at section 3 since law school. I initially skipped over it when I saw it in the terms of reference for the defamation law reform, but I decided to have another look at it. Lo and behold there is a reference to freedom of expression which I don't think appears anywhere else in any kind of legislation. That's the closest we have to a human right (in section 3 of the Defamation Act) which is slightly ironic. There's also a reference in there to protection for the discussion of matters of public interest. So, it's not just about informing people of those matters, but discussing them, and we don't have that the way the Act is currently being interpreted. I'm hoping that Australia's Right to Know coalition on behalf of all the media organisations, as well as many other voices chiming in on this review, will really effect some substantial changes that could help reinforce those rights that are simply just being disregarded.

**ROSEN:** Do you think the same change is coming for statutory qualified privilege?

**ALICK:** I think so. I certainly hope so. I personally don't know how I would rewrite it but it has to be rewritten and I trust that people wiser than me can work out how to get this right because as it stands it does not work. It is a pointless defence.

**ROSEN:** Another potential reform that has been raised is a single publication rule. What are your views on this?

**ALICK:** As the law currently stands, every time an online story is accessed by a reader another act of publication occurs. Where that really bites is when we have a limitation period that runs for 12 months from the act of publication. So a story that's been sitting on the Sydney Morning Herald website since 2010 would normally have the limitation period expire in 2011, but if someone reads it today we have another act of publication and the limitation period begins again starting from today. What that means in real terms is that, as the Sydney Morning Herald's lawyer, I have to work out whether a story from 2010 was true at the time. Can I prove it true now? Who are the witnesses I can call? Where are the documents that can prove it true? We've had some instances where crucial witnesses have passed away from old age. It's incredibly difficult. At any given time, I have about half a dozen of these cases and they just don't feel genuine – you do wonder if a plaintiff was defamed nine years ago why are they suing now.

**ROSEN:** One of the rationales for the one year limitation period is that most of the damage is done in the period immediately following publication. One could see how this might be slightly different in the Internet age. Do you think the responsibility of publishers in the Internet age is any different? If we have a single publication rule, would you settle for a discretionary component with respect to the limitation period like the UK?

**ALICK:** I think the responsibility is greater. I think that is because of the "searchability" of these records now. For example, if someone commits a crime and that crime is reported in a local newspaper and sits on the website that person's name can be searched online for the rest of their lives. So from that perspective, the circumstances are different in the online age. As for the limitation period, when it comes to online publications I would accept a single publication rule with a discretionary component as to the limitation period as is the case with the *Limitation Act 1980* (UK) – you do need the ability to have things taken down in certain cases.

**ROSEN:** In other news, the Open Justice Review was announced earlier this year. Are there any areas of change that you are hoping for in that review?

**ALICK:** In my experience, suppression orders are being made excessively and out of an abundance of caution which flies in the face of the legislative requirements of the orders. Section 8 of *Court Suppression and Non-Publication Orders Act 2010* has five grounds for making suppression orders. Each one of those grounds is prefaced with the requirement that the order be "necessary" for the purpose. The test of necessity is repeated five times in the section alone and yet it is completely ignored the vast majority of the time. I have heard prosecutors seek suppression orders "out of an abundance of caution", which has been rejected by appellate courts as a basis for making a suppression order. Defence lawyers have also been known to seek suppression orders on this basis – I have even seen defence lawyers try to seek suppression orders for the benefit of the victim. I understand that judges hearing criminal proceedings have an enormous workload, but open justice and the public's right to know are being trampled on by these applications.

**ROSEN:** So you are known in certain circles as the "queen of suppression orders", do you get any time these days to make the case for open justice on your feet?

**ALICK:** Unfortunately I don't get to fight suppression orders these days. I was very fortunate when I was at News Corp as in-house counsel to be able to engage in that advocacy and it was a great experience and one which I wish I had more time for at Nine. It is an incredibly rewarding part of the job fighting for the public's right to know. In my previous role, I used to turn up to court routinely to fight suppression orders and I would win – not because I'm good, but because I turned up and took the time to take the judge through the material and apply the necessity test. Time and time again I would win because the applications for suppression orders should never have been made in the first place.

**ROSEN:** I hear you have quite an impressive track record – how many suppression orders have you been involved in as an advocate?

**ALICK:** Over a hundred and I have won every single one. I became very confident at it, not because I am a genius – it's not brain surgery – it's about applying the authorities and looking at the wording of the section and applying it. These orders are wrongly made because the lawyers and the judges don't have time to go through them. If someone from the media has the time and the money to turn up and oppose them, we win every time. Of course, it takes time and money to launch a review or appeal of a suppression order. As media organisations we frankly just don't have the resources anymore to have these kind of fights regularly.

**ROSEN:** You hear about the number of suppression orders that are made by the courts (Victoria wins by a mile), how do you keep on top of them?

**ALICK:** It's practically impossible. At least in Victoria there is a three day notice for the media prior to the orders being made. In NSW, we have ad hoc notification after the fact. If a judge remembers to tell the media officer of a court to inform media organisations of a suppression order, we will then get an email. Often the suppression orders are meaningless to us. For example the order will be made in respect of the individual named in an affidavit to which we don't have access.

**ROSEN:** Do you think suppression orders have a place in this day and age when publishers beyond the jurisdiction take no heed of them?

**ALICK:** The internet poses many challenges for the law and this is just one of them. We have orders being made by courts, often baselessly, to suppress information. The internet hates suppressing information.

It has always had a mantra that information should be free. We have seen Wikileaks publish suppression orders where the order, which contained a list of names, was itself suppressed in the Reserve Bank Securency and Note Printing Australia case. I was part of an application, on behalf of News Corp, to have the order revoked on the basis of futility, which was successful. Justice Hollingworth of the Victorian Supreme Court agreed that the internet publication had made the order futile.

**ROSEN:** It seems that we have in the past respected suppression orders made beyond our shores – for example in the English PJS v News Group Newspapers ([2016] UKSC 26) case, the Americans took the story and ran with it, but the Australian press seemed to respect the privacy injunction (at least online). As in house counsel what is your approach to these kinds of issues?

**ALICK:** We respect them notwithstanding that they are made in another jurisdiction The threat of going to jail, as we all know, in these types of cases is very real. I also think the legislative framework in Australia operates to create a certain degree of self-censorship.

**ROSEN:** Speaking of which, the most recent AFP raids have come as quite a shock. What are your thoughts in the wake of the scandal which has made headlines around the world?

**ALICK:** The raids by the AFP are extraordinary. Previously, the AFP raided Seven Network in relation to allegations that Chappelle Corby had sold her story to the network. But the recent raids are on a completely different level. This is raiding a media organisation and the homes of journalists to seek documents relating to stories that are in some cases three years old where the source of the material appears to be a government employee who leaked the material to the journalist. This intimidates whistle-blowers and journalists. I do not see what the purpose of the raids could have been. Why on earth would a journalist have confidential documents in her underwear drawer, in her house, years after the story ran? These are raids by authorities that can presumably check their own employees' email records and have a fair idea of which employees had access to the leaked documents. The suggestion that they had nowhere else to begin than raiding the ABC years after the story ran is ridiculous. It has made Australia a laughing stock around the world. There is nothing more embarrassing than reading the BBC coverage of this. And it is little attacks like this (which we as Australians try to downplay and be cool about) that will slowly erode what little rights we have to free speech and to know when governments are involved in wrongdoing.

**ROSEN:** On behalf of CAMLA and the Young Lawyers Committee, thank you Larina.

**Antonia Rosen** is a CAMLA Young Lawyers representative and lawyer at Banki Haddock Fiora.

# **Still Phishing:** The Notifiable Data Breaches Scheme One Year On

**Rebecca Lindhout**, Special Counsel, and **Andrew Miers**, Partner, HWL Ebsworth Lawyers,
**reflect on the OAIC's Notifiable Data Breaches Scheme 12-Month Insights Report.**

## Key Points

- The Notifiable Data Breaches Scheme 12-month Insights Report issued by the Office of the Australian Information Commissioner (**OAIC**) on 13 May 2019 (**Annual Report**) revealed that malicious or criminal attacks which exploit vulnerabilities involving a human factor continue to be the main reasons for notifications under the Notifiable Data Breaches Scheme (**NDB Scheme**).
- According to the Annual Report, phishing and spear phishing are the most common and highly effective methods by which entities are being compromised - whether the entity is large or small, and within Australia and internationally.
- The OAIC's findings are broadly consistent with our experiences in handling data breaches during the first 12 months of the NDB Scheme. In particular, the impact of phishing emails, often resulting in business email compromises, dominate the cyber incident landscape.
- While entities generally appear to be taking steps to comply with their obligations under the NDB Scheme, the OAIC notes that there is still an opportunity to be more proactive in approaching privacy and data security compliance and to build further trust with individuals, particularly in relation to harm minimisation and prevention of further data breaches.
- As a result, we recommend clients take this opportunity to review and update their approach to data security and handling data breaches including prevention, harm minimisation and their notification procedures, particularly based on the observations and recommendations of the OAIC.
- We also recommend clients seek expert advice in dealing with data and cyber breaches and, if they have a cyber insurance policy, engage with their insurer in responding to any breach, including any breach response solution the insurer may offer.

**Continued on page 8 >**

## Snapshot of the statistics

| | |
|---|---|
| **Volume of notifications** | As expected, the introduction of the NDB Scheme resulted in an increase in notifications of data breaches.<br>• The OAIC received 1,132 notifications in total, of which 964 were eligible data breaches (for which notification was mandatory) and 168 were voluntary (either because they were not 'eligible data breaches' under the NDB Scheme or because the reporting entity is not bound by the Privacy Act).<br>• This was a 712% increase in data breach reporting compared with the previous 12 months under the voluntary scheme that existed prior to the NDB Scheme.<br>Reporting was fairly consistent during the year with 242 notifications during April - June 2018, 245 notifications from July - September 2018, 262 notifications from October - December 2018 and 215 notifications from January - March 2019. |
| **Cause of data breaches** | Of the reported data breaches:<br>• 60% were caused by malicious or criminal attacks;<br>• 35% were caused by human error such as incorrectly addressed emails and lost data storage devices; and<br>• 5% were caused by system faults such as a bug in the web code.<br>Malicious intent was the primary motivation behind most data breaches, with:<br>• 68% attributable to common cyber threats such as phishing, malware, ransomware, brute force attacks and other forms of hacking; and<br>• 32% attributable to theft of paperwork or data storage devices, social engineering or impersonation.<br>While the report distinguishes between data breaches caused by 'malicious or criminal attacks' and those caused by 'human error', it is worth noting that human error still plays a significant role in most malicious or criminal attacks as well. For example, while phishing incidents are initiated by a malicious actor, they only succeed when an employee falls for the trick and clicks on the offending link or enters their credentials.<br>Our experience of handling data breaches suggests that phishing emails, often leading to business email compromises, are rife in Australia. The Australian Cyber Security Centre has described business email compromise as the 'major current cybercrime threat to business'. Apart from the potential for unauthorised access to personal information, business email compromise also often results in other significant business risks such as the sending of fraudulent payment requests. |
| **Affected data** | The most commonly compromised data is contact information, being 86% of personal information affected by data breaches. Often this will be in combination with other forms of data and it is that combination that can lead to the potency of the potential harm. |

## Key learnings

### Reducing the risk of credential compromise

Credential compromise includes phishing attacks which accounted for 39% of cyber incidents during the first year of the NDB Scheme. Phishing is where confidential information is stolen by sending fraudulent emails to victims. This becomes 'spear phishing' (i.e. more targeted phishing) when individuals or companies are specifically targeted based on company information sourced from publicly available sources such as annual reports and media releases.

To reduce the risk of credential compromise, the OAIC recommends that entities:

- educate users on how to detect phishing emails and about password re-use and security measures;
- implement multi-factor authentication and anti-spoofing controls such as DMARC or SPF; and
- refer to their further guidance about preventing credential compromise.

We also recommend that entities:

- rethink how they effectively secure the types of personal information they hold, including by implementing the Australian Cyber Security Centre's "Essential Eight" Strategies to Mitigate Cyber Security Incidents;
- develop a cyber security policy (and then regularly review and update it);
- prepare a cyber incident response plan (including incorporating a data breach response plan); and
- consider cyber security insurance to offset the cost of responding to cyber incidents and data breaches and potential losses that may arise. An entity's cyber insurance policy will also often provide a breach response solution to assist in responding to an incident.

### Managing Data Breaches

#### *Putting individuals first*

According to the Annual Report, one of the key areas where there is room for improvement is in putting individuals first.

IDCARE (a not-for-profit charity supporting individuals in Australia and New Zealand with identity and cyber security concerns) contributed to the Annual Report and noted a disparity between:

- the time taken between a data breach and misuse of those credentials (9.55 days);
- the average time taken for a breach to be detected (90 days); and
- the time then taken for individuals to be notified (a further 28.25 days).

IDCARE also notes a customer experience score of only 4.1 out of 10 for those affected by data breaches.

In light of the IDCARE insights into how quickly credentials are misused, time is clearly of the essence in both detecting breaches and notifying individuals so they can take preventative action to protect themselves. It is also key to notify individuals in plain English to minimise confusion and enhance trust as much as possible. The OAIC has included additional guidance on how to notify individuals and what to include in notifications in its guide to managing data breaches.

In our experience in dealing with data breaches, this also needs to be balanced against the desirability of not causing undue panic, the guiding principle perhaps being described as 'be alert but not alarmed'.

#### *Assessing the seriousness of harm in relation to a data breach*

The OAIC noted that determining whether a data breach is an 'eligible data breach', particularly the likelihood of serious harm, is still a challenge for entities, particularly where the nature of the harm is less immediate but may still be serious. For example:

- breaches involving contact information may result in that information being used in a phishing attempt which seems more real and so is more successful;
- breaches involving contact information may result in threats to an individual's safety (such as where a person who is the subject of domestic violence has their new address mistakenly disclosed to their attacker); and
- breaches of personal information such as health information may result in damage to reputation or relationships or in workplace or social bullying.

Accordingly, the OAIC recommends taking a longer term approach to monitoring and responding to the risk of harm to affected individuals in the case of data breaches.

In our experience, the possibility of contact information being used in phishing attempts is one of the more common forms of potential harm to arise. However, a breach of contact information is also one of the more nebulous breaches to pin down in assessing the risk of harm since the potential impact is far more indirect and requires other intervening steps first to occur before any actual harm materialises.

#### *Managing multi-party breaches*

Eleven multi-party breaches were reported to the OAIC during the 12 months. A multi-party breach occurs where one or more entities hold personal information jointly - such as where it is owned by one entity and used by others. In these circumstances, each of the affected entities has obligations under the NDB Scheme but compliance by one entity will generally be taken as compliance by each of the entities who hold the information.

The OAIC suggests that the entity with the most direct relationship with the individuals affected by the data breach should make the notification. We think this stands to reason because, regardless of which third party might be responsible for the breach occurring, ultimately it is the reputation of the entity in direct relationship with the individuals whose reputation is on the line. That entity is going to want to have some control over the messaging.

Accordingly, the OAIC recommends that:

- entities should ensure their contracts with suppliers (and other third parties) who have access to and use of their information address arrangements in the event of a data breach. This includes responsibility for gathering the relevant information, allowing access to premises and systems, responsibility for assessing the data breach, taking steps necessary to minimise the harm and prevent it recurring, and also responsibility for making any necessary notifications; and
- entities' data breach response plans should be consistent with the approach they agree in their third party contracts. Data breach response plans should also consider any international notifications which may also be required (eg under the GDPR).

Taking these steps will help:

- minimise the likelihood of multiple notifications being made to the OAIC and to affected persons, which is likely to result in unnecessary confusion; and
- allow entities and their suppliers (or other affected entities) to work in a collaborative manner which gives comfort about transparency and is also more likely to result in harm reduction.

***Harm reduction and preventative measures***

The Annual Report contains practical examples of actual breaches and drawn out suggestions from those breaches around harm reduction and preventative measures which can be implemented in the case of a data breach. These include:

- where an employee's email account was compromised:
  - engaging an external firm to notify affected individuals, including advice to delete the phishing email, change their passwords and monitor their bank accounts; and
  - implementing multi-factor authentication, a secure customer relationship management system for document transfer and additional staff training around spotting spoofed emails as preventative measures; and
- where an entity became aware that an unknown third party had gained unauthorised access to some member accounts in its online portal:
  - immediately notifying the individuals and deactivating the affected accounts;
  - only reinstating the affected accounts with additional security measures such as CAPTCHA (i.e. "completely automated public Turing test to tell computers and humans apart") and identity verification checks to prevent future unauthorised access; and
  - where a data breach affected a vulnerable segment of the community, the affected entity used social workers to notify and provide support to affected individuals via phone.

## Conclusion

The OAIC concluded that *'the first year of the NDB Scheme has resulted in welcome improvements in transparency and accountability for the protection of personal information'*. With plenty of lessons and recommendations coming out of the first year of the NDB Scheme, including those set out above, entities who focus on achieving an environment where privacy and security are core focuses rather than just a 'compliance issue' have the opportunity to enhance trust with their consumers and end-users, and differentiate themselves.

## 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**

# **The View:** AFP Raids

**Paul Fletcher, Communications Minister** (The Australian, 13 June 2019):

"What we want to do is approach this matter in a sober and consultative and calm fashion. As the Prime Minister has said, we're always open if detailed analysis reveals that there's a need for further improvement in the laws."

**Peter Dutton, Home Affairs Minister** (2GB, 6 June 2019):

"Obviously it's a serious breach of our laws when highly classified documents are leaked and the Secretary of the Defence Department makes the decision then to refer that to the federal police. From what I understand of the facts, we're talking about highly classified national security documents, and they were leaked from the department. That's a matter that obviously the Defence Department takes very seriously.

All of us support freedom of the press. If the law needs to be modernised you can have that discussion."

**Kristina Keneally, Senator** (The Australian, 13 June 2019):

"The raids that we saw last week demand that all of us in the community - parlimentarians and media organisations - have a very hard look at the national security framework we have in place. It is fundamentally important that we keep Australians safe, but it is also fundamentally important to our democracy that we uphold one of its most basic tenets, and that is the freedom of the press."

**Arthur Moses SC, Law Council of Australia president** (Lawyer's Weekly, 6 June 2019):

"The role of the media as the fourth estate to assist in the public right to know in relation to matters concerning the Parliament, the Executive and the judiciary must never be underestimated. The media must be able to lawfully report on matters of public interest without fear or favour and, where needed, hold the parliament, the executive and judiciary to account. Any chilling effect on this role would be contrary to the governmental transparency and integrity Australians expect. Sunlight is the best disinfectant when there is public scrutiny of the actions of government by the media."

**Chris Flynn, Gilbert + Tobin partner and legal spokesperson for the Alliance for Journalists' Freedom** (Lawyer's Weekly, 6 June 2019):

"In any democracy, journalism that covers any plan by government departments to allow government agencies to monitor the lives of ordinary citizens is of the highest public interest. As is public discussion of government proposals that affects or limits freedom of private communication between citizens. These raids run the risk of further stifling press freedom in Australia. They reinforce the need for a Press Freedom Act to protect press freedom and free and open debate, and strike and the right balance between those things and our national security framework."

**Emily Howie, Human Rights Law Centre legal director** (Lawyer's Weekly, 6 June 2019):

"New espionage laws criminalise journalism and put us all at risk. These raids highlight just how dangerous it has become to reveal information in the public interest if it also touches on anything supposedly linked to national security. It's outrageous that journalists and their sources could face life imprisonment for revealing information that ultimately protects us all. There are insufficient safeguards to prevent law enforcement agencies from using these powers to expose journalists' confidential sources. This is shocking for those who are targeted but this surveillance also has a chilling effect on people coming forward. We need urgent law reform to stop punitive investigations and instead encourage truth-telling.

Without a free press, we don't have democracy. We don't know what our government is doing behind closed doors. These people should be lauded for revealing the truth but instead they face the real possibility of prison time."

**Kerry Weste, Australian Lawyers for Human Rights president** (Lawyer's Weekly, 6 June 2019):

"The United Nations Human Rights Committee has made it clear that a free, uncensored and unhindered press is essential in any society to ensure freedom of opinion and expression and the enjoyment of other universal human rights. The ability to share information on matters of public interest and to scrutinise government is a fundamental pillar of a democratic society. This can only happen if journalists can access information that is in the public interest and at the same time keep their sources safe and confidential.

The fact that the investigations of Annika's home, computer and phone and of the ABC offices occurred so long after the relevant publications must raise questions about the purpose of the raids.

Australia campaigned for its seat on the United Nations Human Rights Council on the basis that it is an 'international human rights leader' with 'respect for democracy and the rule of law.' Yet we remain the only Western liberal democracy without any federal Human Rights Act to protect rights like freedom of expression. We must ensure that measures designed to protect national security do not diminish our democracy. Legislation must provide a proportionate, necessary and reasonable response to the perceived harms the government seeks to address. When we abandon key democratic principles, such as a press that is free to report on matters of public interest without the journalist and their source being treated as possible criminals, then it is us and not the terrorists who will have damaged our own way of life and undermined our democracy. We must think about the kind of society we want before removing our democratic checks and balances in the name of 'national security'."

**Ita Buttrose, ABC Chair**
(statement, 7 June 2019):

"On behalf of the ABC, I have registered with the Federal Government my grave concern over this week's raid by the federal police on the national broadcaster.

An untrammelled media is important to the public discourse and to democracy.

It is the way in which Australian citizens are kept informed about the world and its impact on their daily lives.

Observance of this basic tenet of the community's right to know has driven my involvement in public life and my career in journalism for almost five decades.

The raid is unprecedented — both to the ABC and to me.

In a frank conversation with the Minister for Communications, Cyber Safety and the Arts, Paul Fletcher, yesterday, I said the raid, in its very public form and in the sweeping nature of the information sought, was clearly designed to intimidate.

It is impossible to ignore the seismic nature of this week's events: raids on two separate media outfits on consecutive days is a blunt signal of adverse consequences for news organisations who make life uncomfortable for policy makers and regulators by shining lights in dark corners and holding the powerful to account.

I also asked for assurances that the ABC not be subject to future raids of this sort. Mr Fletcher declined to provide such assurances, while noting the "substantial concern" registered by the Corporation.

There has been much reference in recent days to the need to observe the rule of law.

While there are legitimate matters of national security that the ABC will always respect, the ABC Act and Charter are explicit about the importance of an independent public broadcaster to Australian culture and democracy.

Public interest is best served by the ABC doing its job, asking difficult questions and dealing with genuine whistle-blowers who risk their livelihoods and reputations to bring matters of grave import to the surface.

Neither the journalists nor their sources should be treated as criminals.

In my view, legitimate journalistic endeavours that expose flawed decision-making or matters that policy makers and public servants would simply prefer were secret, should not automatically and conveniently be classed as issues of national security.

The onus must always be on the public's right to know.

If that is not reflected sufficiently in current law, then it must be corrected.

As ABC Chair, I will fight any attempts to muzzle the national broadcaster or interfere with its obligations to the Australian public.

Independence is not exercised by degrees.

It is absolute."

**David Anderson, ABC Managing Director**
(Lawyer's Weekly, 6 June 2019):

"This is a serious development and raises legitimate concerns over freedom of the press and proper public scrutiny of national security and defence matters. The ABC stands by its journalists, will protect its sources and continue to report without fear or favour on national security and intelligence issues when there is a clear public interest."

**Christian Porter, Attorney-General**
(ABC's Radio National, 5 June 2019):

"This is an investigation from the AFP. I haven't received yet a briefing on it myself. I had no idea it was going to happen, and that's because these matters are totally independent of the executive government.

It's usually the case that in matters that are sensitive – and clearly this is – that there'll be a

quick briefing to alert someone that it's going to happen, when they're the responsible minister, so I would guess...that the Minister for Home Affairs would have had such a heads up immediately beforehand. But the idea, seriously, that the Morrison government or any minister in the Morrison government was somehow involved in the investigation, or the decision, or the timing of the decision, I mean it's absolutely absurd."

**AFP statement** (5 June 2019):

"The AFP's role is to investigate breaches of Commonwealth criminal law. When the AFP receives referrals it assesses them for criminality and does not make value judgements on the issue instead identifying whether there has been any contraventions of Commonwealth Law, and when evidence as to whether the offence has been committed or otherwise.

AFP investigators are required to assess all the relevant facts in every matter. This includes enquiries into the classification of the information concerned, how it was handled and who had access to it. The execution of search warrants is an important tool to our investigations to achieve this but is just one aspect of our work. There are many avenues of inquiry and tools available to the AFP in investigations such as this."

**Campbell Reid, group executive for corporate affairs, policy and government relations at News Corp Australia** (The Australian, 12 June 2019):

"The dangers associated with the ever-expanding dossier of laws that can put journalists in jail has been raised repeatedly with governments and politicians over the past decade. This is not a matter where we need an inquiry to identify the problem.

The government should stop ignoring what it has already been told. Rather than an inquiry, a better solution would be a working group of senior politicians, media representatives and legal experts to work together to reframe legislation so it strikes the right balance between national security and the nation's right to know."

**Peter Bartlett, veteran media lawyer and partner at MinterEllison** (The Australian, 8 June 2019):

"If the ABC publishes something today which the AFP takes the view is clearly a breach, they should raid tomorrow. Why did they wait two years? ... There needs to be a media exemption where if a reporter acts reasonably and in the public interest, then they're protected."

**British Broadcasting Corporation statement** (5 June 2019):

"This police raid against our partners at ABC is an attack on press freedom which we at the BBC find deeply troubling. At a time when the media is becoming less free across the world, it is highly worrying if a public broadcaster is being targeted for doing its job of reporting in the public interest."

**Daniel Bastard, Asia Pacific head of Reporters Without Borders** (SBS, 5 June 2019):

"Persecuting a media outlet in this way because of a report that was clearly in the public interest is intolerable. This kind of intimidation of reporters and their sources can have devastating consequences for journalistic freedom and independent news reporting."

**George Williams, Dean of Law at the University of New South Wales.** This is developed for CLB from an article published in the Australian.

"Australia leads the world in enacting national security and counterterrorism laws. Some 75 have been passed by our federal Parliament since 11 September 2001. This far exceeds the number of similar laws passed by the United Kingdom and the United States. Our laws also differ because they go further in heightening government secrecy.

The focus over recent days has been on laws that permit the police to seize data and documents from journalists in aid of prosecuting people who reveal government secrets. Many laws now permit this. For example, section 35P of the ASIO Act makes it a criminal offence to disclose information about special intelligence operations in which ASIO officers are granted immunity from civil and criminal liability. A person can be jailed for up to five years merely for disclosing information about such an operation. There is no exception for reporting in the public interest.

Of even greater concern are laws that undermine media freedom in secret. One example is the ability of enforcement agencies to access the metadata of journalists, including things like mobile phone records. This information can be accessed to identify the source of a media story without notifying the journalist. The information can then be used to prosecute people who have supplied information to the journalist.

Another example is the power held by ASIO allowing it to compel any person, including journalists, to answer questions for the purpose of gathering intelligence. A person may even be detained in secret

for up to a week. A journalist will face jail for up to five years if they fail to answer every question put to them. Any person who writes or tweets about the use of this power faces another five year jail term.

I could go on with other examples, many of which have been forgotten once the debate over each law died down. These laws through remain in force, and can be used at the discretion of the authorities. Put together, their impact and scope is shocking in showing how far media freedom has deteriorated.

We can thank our politicians for these laws. They have used the fear of terrorism and threats to community safety to enact laws that shield government from scrutiny. Our liberties have had too few defenders. Each of the laws that restrict media freedom and freedom of speech have been passed with bipartisan support. Parliament has long ceased to be the protector of our democratic rights.

Australia's legal landscape has made this possible. We are the only democratic nation without strong national protection for freedom of speech and of the press. The best we have is an implied freedom of political communication derived from our Constitution. It though has been applied rarely by the High Court, and is likely to be of limited value where national security and the media are concerned.

We lack anything like the First Amendment to the United States Constitution, which states in unequivocal terms that 'Congress shall make no law … abridging the freedom of speech, or of the press'. Nor do we possess the protections of free speech found in the United Kingdom Human Rights Act 1998, Canadian Charter of Rights and Freedoms 1982 or New Zealand Bill of Rights Act 1990.

Laws like this make a difference. They counterbalance the desire of governments to keep embarrassing and damaging material secret. They also provide legal backing to the media in reporting such information. If we want to avoid more raids and the further erosion of media freedom, we must convince Parliament enact long overdue protection for freedom of speech and of the press."

**Prof Peter Greste, Unesco chair in journalism and communication at the University of Queensland, and a founding director of the Alliance for Journalists' Freedom**
(The Guardian, 6 June 2019):

"Recent raids by the Australian Federal police on the News Corp journalist Annika Smethurst and the ABC are a serious threat to the most fundamental role that the media plays in a democracy.

By definition, democracy is government by the people. Politicians act on behalf of those who employ them; that is, us Australian voters and taxpayers.

As their employers we have both a right and a responsibility to know what is being done in our names. The means by which that is done is through good journalism.

Of course, there are things that governments need to keep secret. Whether they are the financial or health records of private citizens, or the operational details of our security services, there are places that nobody outside of the agencies involved should have access to. But what happens when things go wrong? What happens when someone abuses the power or authority that we, the voters, have invested in them? What happens when the internal mechanisms of accountability and transparency break down? Or when government officials use the cloak of "national security" to cover up something that we all ought to know about and debate in public?

The tool we recommend is a media freedom act that positively puts the role of the press in the middle of our legal system. At the moment, there is nothing in Australian law that explicitly protects press freedom in the way that the first amendment does in the US constitution.

Such an act would recognise the fundamental importance of national security and the protection of certain commonwealth activities and the identities of key employees, while still providing a basis for journalists to investigate and report on government misconduct.

More than simply making reporting "in the public interest" a defence, it would make it an exception from prosecution. That isn't to suggest that journalists would be immune, but the onus would be on the security agencies to show that the exception of "public interest reporting" does not apply, before charges are laid. In effect, it restores the assumption of innocence which the current legislation has overturned.

There is no evidence that the journalists that the AFP targeted over the past few days did anything that genuinely damaged national security. Rather, those journalists exposed issues that we needed to know about, needed to debate and in some cases needed to change.

To be clear, this is not simply about protecting the rights of journalists to stick their noses into the inner workings of government. This is about ensuring the kind of transparency and accountability that has helped make Australia one of the most stable, prosperous and peaceful places on the planet."

**Geoffrey Robertson QC, human rights barrister** (SMH, 8 June 2019):

"What an irony. As the free world celebrates D-day and the heroes who kept it free from the Gestapo's "knock on the door", the international news on the BBC leads with the spectacle of the police raid on the ABC offices.

This could not happen in other advanced democracies, which all have constitutional protections for journalists and their sources of information, although of course it does go on in Istanbul and Rangoon – and now in Sydney. How did we become so out of sync on press freedom, invasions of which are the sign of a second-rate country?

This week's raids have diminished Australia's international standing, so Parliament must at least make amendments requiring police to obtain the DPP's approval before any future attack on the media and requiring them to make an application to a real judge which the media can contest before any action is taken.

The behaviour of the AFP should be put under intense scrutiny by Parliament. Did it take legal advice before it applied for a warrant and from whom? Did it consider that the ABC had an obvious public interest defence? Does the AFP not consider the alleged murder of civilians by the Australian army is a matter of public interest? The ABC program went out in 2017. Why the long delay if national security were really at stake? What if anything did police tell the court registrar? The source of the leaks, former military lawyer David William McBride, identified himself in March when he said he would defend charges on the grounds he had a duty to report the information. The leaker identified, were not the raids on the ABC entirely unnecessary?

And why did the AFP consider it necessary to ransack Smethurst's home? If these and many other questions are not answered satisfactorily, then heads should roll."

**Bret Walker SC, a former Independent National Security Legislation Monitor** (SMH, 11 June 2019):

"I have no patience whatever for the idea that there is no such thing as a national security secret - I think there are many things which need to be kept secret for the purposes of national security.

Whistleblowing is there because bad things do happen in government. Government is composed of people and people do bad things.

In a democracy ruled by law, we should be welcoming, not persecuting, the release of information ultimately to the public ... about suspicions of wrongdoing in government, so long as those suspicions are formed in good faith."

**Joe Hildebrand, journalist** (news.com.au, 9 June 2019):

"I don't have the slightest problem with federal police raiding journalists at News Corp and the ABC. In fact, my only concern is how they did it.

If the AFP were going to be truly fair dinkum, then they should have slicked back their hair, slapped on a leather jacket and strapped on a pair of waterskis.

Because these guys have just jumped the shark.

Indeed, of the approximately 250,000 or so words in the English language there is probably not one that adequately conveys how utterly stupid the raids are, nor how utterly certain they are to backfire against the very objective the security agencies are trying to achieve."

**Kate McClymont, SMH investigative journalist** (Twitter, 5 June 2019):

"Why wait two years to investigate this? Again, the crucial question is the complainant. Police don't raid without someone lodging a formal complaint. Two media raids in two days is not a coincidence."

"My take, for what it's worth, is that in a perverse way the AFP raids have been beneficial. They've unified the media, garnered worldwide attention & highlighted the vital service journalists & whistleblowers play in shining a light on things those in power don't want us to see."

**Kerry O'Brien, Walkley Foundation chair and long-time presenter of the ABC's 7.30 program** (ABC Radio, 6 June 2019):

"If they care about democracy, this does go to the heart of democracy and the democratic process.

You are talking about the media going about its job in providing scrutiny to areas of government where scrutiny is not easy.

You are also talking about the role of whistleblowers, who are mostly well-motivated people who are disturbed about what they are seeing inside the Government in this case."

# Israel Folau and Rugby Australia
## A What Not to Do Guide to Mediation About Religious Speech

**Dr Mitchell Landrigan, Adjunct Professor, Faculty of Law, University of Technology Sydney, gives us his thoughts about the strategy adopted in the Folau and Rugby Australia dispute.**

Where there is a dispute, there is conflict. Rugby Australia and Israel Folau were (and still are) in dispute about Folau's April 2019 Instagram post. The matter is seemingly destined for the courts. Yet, courts and quasi-judicial tribunals are generally *not* effective forums for resolving conflict. They are forums for deciding upon, and ruling on, points of law after judges or tribunal members review facts and receive submissions from lawyers. Their decisions are binary. Rugby Australia's own procedures directed the Folau dispute to a specialist tribunal hearing. A tribunal of three found Folau to have committed a 'high level breach' of the Code. That appears to be the full extent of any formal dispute resolution about the limits of Folau's religiously motivated speech.

There are better (and cheaper) methods of dispute resolution than decisions by courts and tribunals. Consider, for example, dispute resolution by mediation. A skilled mediator can help parties to articulate their 'interests' rather than only their opposing 'positions'. A well-conducted mediation with a skilled mediator (or more than one mediator, if considered necessary) can be a more effective method of resolving disputes – and with longer lasting more beneficial effects - than a binary tribunal ruling. Mediation can involve multiple parties, each expressing and, crucially, listening to, and understanding, the perspectives of others. It is the antithesis of quasi-judicial proceedings where arguments are presented (by lawyers) in a setting of legal conflict.

Mediation between Folau and Rugby Australia (possibly involving other stakeholders such as sponsors) could have given Folau an opportunity to explain to affected parties (say members of the LGBTIQ+ community) his perspective on his expression and, likewise, for affected parties to explain to him the possibly hurtful effect of his speech on them. The participants could have *learnt* from each other about the motivations for, and effects of, provocative and potentially hurtful religious speech. It is, of course, possible that no mediation would have been effective in resolving these differences because the parties would under no circumstances be prepared to explain their interests to each another. However, interest-based dispute resolution seems to have not been given a chance. It is as though Rugby Australia considered the Folau message to be so polarising that Rugby Australia forgot how to engage in dispute resolution other than via litigation.

It is useful to provide some background to the Folau saga. This starts on 4 April 2018. Upon tearing a hamstring, Folau wrote a biblically themed message on Instagram about his 'trials'. He responded to an online question (addressed to himself) about what happens to gay people. Folau's message at the time was similar to the one he would post on Instagram on 10 April 2019, and which would lead to his sacking. He said gays would go to hell.

Folau reportedly met in April 2018 with Rugby Australia's representatives, including Rugby Australia's chief, Raelene Castle, to discuss Rugby Australia's concerns about the post. After the meeting, Castle addressed a press conference. While referring – pointedly - to the importance of rugby players respectfully using social media, Castle announced that Rugby Australia was proud of Folau for standing up for his religious beliefs. Castle also said that Folau had accepted at the meeting that he could have put a more 'positive spin' on his Instagram message and that he had acknowledged at the meeting that he could have conveyed the same message less disrespectfully.

It is not clear whether Castle understood the implication of her describing Folau as being an ineffective spinner of religious beliefs. A man who believes in biblical inerrancy is unlikely to react with pleasure to the notion that he conveyed a biblical message with insufficient 'spin'. Folau soon expressed his disappointment online about the message Castle conveyed at the press conference. He disagreed with her version of events. This apparent disparity of understanding between Folau and Castle about the content of 2018 meeting suggests there was no concerted effort by Rugby Australia to agree with Folau and document at the conference what Rugby Australia would

communicate afterwards. It also likely pointed to future problems in the relationship. Rugby Australia nevertheless extended Folau's playing contract for four years in late 2018, reportedly sans a social media clause.

Folau again posted a message on Instagram on 10 April 2019, condemning homosexuals to hell. It is not obvious what (if any) concern or event prompted Folau's message. His post relegated various classes of persons to hell, including homosexuals. The message could have been deeply hurtful to members of the LGBTIQ+ community (if not necessarily the atheists, who were included in the extended catalogue of sinners). Folau *may*, it should be said, have intended his message to be a positive one and to not be merely condemnatory of gay and lesbian people: he urged such people to repent. This message of repentance, however, connotes sinfulness. Even if possibly well-intentioned, this aspect of Folau's message may have exacerbated its offensiveness and hurtfulness.

Rugby Australia announced publicly, and swiftly, that Folau's online comments breached the players' Code of Conduct and that it would seek to terminate Folau's four-year employment contract. Michael Cheika – the Wallabies head coach – lamented publicly, and precipitously, that he would not be able to select Folau in the national team. Within little more than a month of the April 2019 Instagram post, Rugby Australia and Folau had appeared before a specially convened Rugby Australia tribunal hearing, before three independent experts. The tribunal handed down its ruling. It recommended that, because Folau had committed a high-level breach of the Code (and had shown no remorse or willingness to retract the post), the appropriate action from Rugby Australia was to terminate Folau's contract. It is unclear why the tribunal chose to place any significant weight on Folau's lack of remorse, given that, in 2018, Castle had commended Folau for holding steadfastly to his religious views.

In May 2019, Rugby Australia announced that it would terminate Folau's contract. In June 2019, Folau launched a website to raise money to pay for the legal costs of his looming litigation with Rugby Australia. This website (having reportedly raised $750,000 in four days) was 'taken down' for allegedly breaching GoFundMe's terms of service; the site also appears to have been the subject of a denial of service attack. The Australian Christian Lobby offered to host an alternative crowdsourcing site for Folau and it pledged $100,000 towards his legal costs. In less than a day, its alternative crowdsourcing site had raised more than one million Australian dollars for Folau.

In the meantime, Folau's wife, Maria Folau, a netballer who represents the New Zealand national team Silver Ferns and now plays for the Adelaide Thunderbirds, reposted her husband's GoFundMe plea. This led to Netball Australia and Super Netball issuing a joint statement defending netball's inclusiveness. Netball South Australia shared its views about Maria Folau's reposting of her husband's plea, stating that, while Netball South Australia did not endorse the Maria Folau reposting, it did not believe that Maria Folau's endorsement of her husband's plea contravened any social media policy. ANZ, a sponsor of the Silver Ferns stated publicly that it did not support Maria Folau's views. In response to ANZ, Netball New Zealand clarified that it, too, valued diversity and explained that it did not consider Maria Folau's reposting of her husband's message to have breached any of its social media policies.

It is not at all obvious how much consideration Rugby Australia gave to the concerns of some of the parties with stakes in the Israel Folau matter and how their interests would be catered for by litigation. This point was none-too-subtly emphasised by several mostly Polynesian Christian rugby players ostentatiously expressing their religious solidarity with Folau through on-field group prayer after games during the 2019 *Super Rugby* season. Nor is it clear whether Rugby Australia ever sought to identify all the parties with possible interests in the Folau dispute (including, a major sponsor of a women's national sporting team in a neighbouring country) and whether these parties might, if given a choice, prefer there to be some attempt by Rugby Australia at private mediation.

It would seem that the interests of few if any stakeholders have been preserved by Rugby Australia's quasi-litigation. First, there are the members and affiliates of Rugby Australia – the rugby clubs, teams and players – who aim (or should aim) to be inclusive of all their members, irrespective of members' sexuality or beliefs. Folau's sacking sends a strong message to the clubs, teams and players (including his own former *Waratahs* and *Wallabies* teammates), that homophobic expression will not be tolerated. But termination of an employment contract after a tribunal decision is a blunt outcome. Those clubs, teams and players include members with strong beliefs (such as some of the Polynesian players).

Some members may now wonder about the limits of any public expression of their *own* views. Rugby Australia has not explained how people can respectfully express their religious views within a sphere of tolerable provocativeness. Rugby Australia has also, in my view, not provided the public with a

compelling narrative to account for its sacking of Folau. It could have been no more complicated than Rugby Australia explaining that it does not support its paid players publicly (cf *privately*) using religious speech to morally denounce minorities such as the LGBTIQ+ community and/or to publicly (cf *privately*) equate LGBTIQ+ people with drunks, adulterers, liars, thieves, fornicators and idolaters. Rugby Australia's sacking of Folau will also not deter him from publicly expressing similar views as an unemployed – yet still famous – former sporting star. There is the potential for Rugby Australia's termination of Folau's contract to turn Folau into a modern-day martyr of bureaucratic opposition to free religious expression. It is of note that the Anglican Archbishop of Sydney, Dr Glenn Davies, has declared Folau's 'right' to religious expression to be 'vilified'. Folau's public following may continue to grow. So may his frustration.

Secondly, there are the members of the LGBTIQ+ community, who should – rightly – take strength from Rugby Australia's strong stance against potentially harmful, even homophobic, statements from a high-profile sportsman. Yet, even some members of that community may now wonder about the limits of their own free expression and they, like rugby's sponsors, have now lost the benefits of watching a player who, at his best, is one of rugby's great players.

Thirdly, as suggested, there are the sponsors of Rugby Australia, including Qantas. The chief commercial interest of rugby sponsors (and of sports sponsors generally) is in the sponsored party – the *Wallabies* or Folau as the case may be - bringing as much economic reward as possible for the sponsor by winning matches or scoring tries. Or at least, *trying* to win games. It is a simple equation. A sponsor has no economic interest in a team (or a player) courting controversy. Alan Joyce, the Qantas CEO, expressed this view pithily when he said 'We don't sponsor something to get involved in controversy. That's not part of the deal.'

At one level, the tribunal proceedings and the termination of Folau's contract would appear to have addressed sponsors' concerns. Yet the outcome pursued by Rugby Australia has likely resulted in the loss to the game, and possibly to sport more generally, of a marquee player. It is hard to conceive of how the termination of a player's contract over his speech could be in the sponsors' *best* interests. A better outcome would be that Folau continued to play for the *Wallabies* (or could be available to play for them) with a mediated agreement in place about his social media posts which *then*, if he breached, could be enforced (perhaps after further mediation). All of which could be achieved without a public dispute about free expression at a time when interest in rugby in Australia is ebbing.

On announcing the termination of Folau's contract 10 days after the decision of the independent tribunal, Castle advised that Rugby Australia was 'left with … no choice but to pursue a course of action resulting in today's outcome'. This statement is telling. It suggests that Rugby Australia did not even consider mediation to be an option.

Mediation – a highly effective form of facilitated interest-based negotiation – can bring parties together with the mutual objective of resolving disputes. It is not necessarily a one-on-one activity; mediations can involve multiple stakeholders with divergent perspectives. A skilled and experienced mediator (or, in some cases, more than one mediator) can help the parties to identify/express their interests and – critically – to understand the values and passions of the others around the table. The process can be slow, and it requires patience. Yet is has the real potential for parties who have seemingly intractably opposing 'positions' to understand the 'interests' of the others and to work towards mutually acceptable, long-term outcomes. A mediation table comprising Folau, sponsors, and representatives of the LGBTIQ+ community could have achieved a better outcome – a potentially more conciliatory one – than the situation Rugby Australia now faces. As noted, the mediation may have failed. Perhaps the parties would have no desire or willingness to listen to, or face, each other. In this case, however, regretfully, mediation as a form of dispute resolution appears to have not even been conceived of.

These are the author's (and only the author's) personal views

# CLB Interview: Anna Johnston

**To celebrate Privacy Awareness Week and the anniversary of the GDPR (we're fun like that here at the *Communications Law Bulletin*), Eli Fisher, co-editor, sat down with Anna Johnston to talk about what's happening in data law.**

By way of a perhaps unnecessary introduction, Anna Johnston is [redacted] Privacy joke. (Tough crowd.)

Anna is one of Australia's most respected experts in privacy law. Anna was a Deputy Privacy Commissioner for NSW, and has been commissioned to write privacy guidance publications and deliver presentations and training on behalf of other regulators including the Australian and Victorian Privacy Commissioners. She established Salinger Privacy in 2004, making wonderful use of her right to use a pseudonym (high five, APP 2!), where she specialises in privacy and data governance issues. She has established herself as a go-to expert for privacy compliance.

Anna has been called upon to provide expert testimony before various Parliamentary inquiries and the Productivity Commission. She is a lifetime member of the Australian Privacy Foundation, a member of the International Association of Privacy Professionals (IAPP) since 2008, and in 2019 was recognised as an industry veteran by the IAPP with the designation of Fellow of Information Privacy (FIP).

**ELI FISHER:** Anna, on behalf of all of our readers, thanks so much for chatting with us. As someone who is working in this area every day, what parts of data law are keeping you busiest?

**ANNA JOHNSTON:** It's a mix of the foundational concepts, and then there's always something new. So in any given week we might be running some basic privacy awareness training for a client, drafting a collection notice or giving advice about allowable data uses, but also perhaps working on a Privacy Impact Assessment of some interesting new technology project, maybe a chatbot, or the establishment of a data analytics centre. But no matter what kinds of projects we are looking at, the basic questions are the same: can and should we collect this data, can and should we use it for this purpose, to whom can we disclose it, and how do we keep it safe?

**FISHER:** I forgot to get my kids Privacy Awareness Week presents this year. What did you do for it? Did you make any PAW resolutions for 2019?

**JOHNSTON:** We did a bunch of things for PAW this year. Salinger Privacy ran a free webinar on behalf of the IAPP about Privacy by Design in Privacy Law, which was fantastic. We had over 500 attendees. Another webinar, on Privacy Law for IT Professionals, was one of our regular series of professional webinars. I wrote a piece for the NSW Law Society Journal about a couple of new cases which impact on employers' liability for the privacy harms caused by 'rogue' employees, I was a member of a panel of speakers for the launch of Deloitte's 2019 Privacy Law Index, and for our monthly blog we focussed on explaining the basics of privacy law as a kind of Privacy 101 (see https://www.salingerprivacy.com.au/2019/05/03/privacy-101/).

**FISHER:** Anna, you were a regulator for a number of years before moving to private practice. Given that the case law in this area is so scarce, and the law is deliberately drafted in terms of principles, it's an area of practice that requires judgment calls. To what extent does your regulator background inform the way you practise? And what can we non-regulators do to hone that instinct?

**JOHNSTON:** The 'fuzzy' nature of privacy law is one of the things I love about it - you do need to use your judgment, and think about what your customers would expect, and what you can do to avoid causing them any harm. Something I have carried with me from my regulator days is a passion for explaining privacy topics to a lay audience. It's easy to get caught up in the minutiae of APP this and exemption that; but mostly privacy law boils down to common sense and good manners. So my advice for lawyers is to be less lawyerly; take a step back and look at the bigger picture. Because the law might say whether your client 'can', but not whether they 'should'. Having said that, there is actually a swag of case law coming out of the NSW Civil and Administrative Tribunal, and keeping on top of that for our annotated guide is how I keep the lawyerly side of my brain functioning.

**FISHER:** There's a real sense, at least from where I'm sitting, that privacy has gone from being a regulatory peripherality to something that businesses, government and regulators, and social commentators are profoundly concerned about. What's changed in your view?

**JOHNSTON:** Things have absolutely changed. I have worked in privacy since 2000, so I have seen the pendulum swing away from privacy concerns in the wake of the September 11 attacks in 2001 and all the focus on surveillance that arose from that, and then massively swing back again in the past couple of years. First there were the Edward Snowden revelations, and then the focus on the GDPR, but the real game changer was the Facebook/Cambridge Analytica scandal, which seemed to reach into public consciousness in a way that hadn't really happening before. You

just look at the shift in tone from Mark Zuckerberg, who first developed Facebook within that post-September 11 anti-privacy mentality of "if you've got nothing to hide...". He's gone from saying about 10 years ago that privacy is no longer a social norm, to last year saying actually it's the most important thing his users value. The OAIC's community attitudes surveys back that up; people are becoming more concerned about their privacy than they were 10 or 15 years ago.

**FISHER:** The GDPR was obviously a very big deal. It's kept a lot of us busy in Australia, and around the world. How did you feel about it when it first came into effect a year ago, and how do you feel about it now? Was it over-hyped, or has it truly changed the game?

**JOHNSTON:** I think the focus on May 25 was over-hyped, as if you had to 'be compliant' by then or the sky was going to fall in. But the long-term reach of GDPR I don't think is over-hyped. It will take a while for the impacts to really lead to business change, but GDPR certainly has the power to reign in the excesses of the data surveillance economy. And then there's the ripple effect; I've just come home from a gathering in Tokyo of privacy regulators from the Asia-Pacific, and there is so much talk about GDPR and how it either directly affects businesses in the region, or indirectly is affecting both consumer expectations and legislators' thinking.

**FISHER:** Do you think that the GDPR has got its extraterritorial focus right? Is it futile trying to regulate privacy by reference to national borders?

**JOHNSTON:** Yes, GDPR works because of its extraterritorial reach. How effective enforcement will be across borders is a live question, but the drafting was deliberate, to catch businesses which previously avoided privacy laws based on their physical location being different to their customer base. Now what matters is the physical location of the affected individuals.

**FISHER:** Do you think that the GDPR has filtered into the way we interpret the APPs? So much of the APPs is based on "reasonableness" – what the individual would reasonably expect you to do with her or his personal information, what level of security you need to adopt, how long an APP Entity can take before performing an obligation. Do you think that the meaning of "reasonable" has shifted in light of stricter GDPR standards?

**JOHNSTON:** I think the interpretation of what is 'reasonable' is shifting all the time, and that's a good thing. It's how privacy law manages to stay relevant to both new technologies and shifts on community expectations. If the law were more prescriptive it would quickly become out of date. But it's not just the GDPR having an impact, that shift in expectations can come from anywhere. There was a recent QCAT case, *ZIL v the Queensland Police Service*, in which

the issue was whether the police service took reasonable measures in terms of data security. I found this case interesting because the Tribunal said that as the community's understanding of and attitudes towards family violence has changed, the community's expectations have increased that the police service will do more and more to protect the privacy (and thus personal safety) of victims of family violence. And that translated into a finding that a failure to prevent unauthorised access to a family violence victim's records, and a failure to monitor access proactively was not good enough anymore. The police service had not taken 'reasonable steps' to prevent the misuse of the personal information it holds. It was explicitly found that while similar cases previously failed, this one succeeded, precisely because community attitudes have shifted. And as a community we now expect more from the organisations which hold our personal information. So what is considered 'reasonable' data security measures is increasing over time.

**FISHER:** It seems like the biggest concern of data management is a data breach. A few months before the GDPR came into effect, Australia got its mandatory data breach notification scheme. Those entities caught by the GDPR got a second layer of data breach notification obligations with that regulation. APRA-regulated entities are now grappling with CPS 234. And of course businesses, whether they're caught by the GDPR, the Privacy Act, CPS 234 or any other data breach notification obligation, will have private contractual obligations regarding notification of breaches which may vary from contract to contract. What is a practical way to manage this tangled melange of varied security standards?

**JOHNSTON:** Organisations need a Data Breach Response Plan, which incorporates each of the rules applying to them. The Plan needs to anticipate who will need to be involved in any breach response, not just the privacy officer but also the risk and compliance team, lawyers, forensic IT investigators, and who needs to be briefed, like your insurer and your media or PR team. The Plan should help the right person make the right decisions at the right time, like the point when you need to assess the level of harm that might arise for affected individuals. The legal tests, and the timeframes for notifying, differ between the Australian and European schemes. The Plan also needs to help everyone in the organisation distinguish between a data breach and a cybersecurity incident; they are not always the same thing, and so your response path will need to accommodate that. And you will need templates at the ready, including a reporting format for the relevant regulators.

**FISHER:** Let's talk bugbears. We all have a few. I know consent drives you nuts, especially the way privacy policies are often wielded. Walk us through it.

**JOHNSTON:** It's the practice of dressing up other things as 'consent', when they are really not, that drives me nuts. If it's a collection notice or buried in a privacy policy, it's not consent. If it's a condition of doing business with you, it's not consent. If I had no genuine choice to say 'no', it's not consent. I describe consent as the "would you like fries with that?" question. If I can freely say no to the fries, but still get the burger I want, without any kind of penalty for saying no to the fries, then if I do say 'yes' to the fries you can call it consent.

**FISHER:** So what are your tips for better managing consent?

**JOHNSTON:** Go back to basics. Don't start from a point of thinking about consent. Instead, think about "are we lawfully allowed to collect, use or disclose this personal information?" There are plenty of grounds under which privacy law allows you to handle personal information in a lawful way, without needing to go anywhere near relying on consent. Consent is not the rule, it is the exception to the rule. But if you have no other lawful ground on which to collect, use or disclose personal information, then seeking the individual's consent is your final option. But know that they need to be free to say 'no', and if they say no then you can't do it.

Privacy policies are important from a transparency perspective. But they are not a tool for seeking anyone's consent.

**FISHER:** Ok, so let's turn to data becoming an antitrust issue. What are your thoughts about the ACCC's inquiry and preliminary report, from a data perspective?

**JOHNSTON:** It's going to be really interesting to see how the final report from the ACCC turns out. I was originally sceptical of the role a consumer protection and competition regulator would play in this space, and I saw the ACCC's involvement as a symptom of the sidelining of the OAIC. (The US model of privacy regulation is to rely on their consumer and competition regulators, and I think that has utterly failed as a regulatory model.) But the preliminary report from Rod Simms was spot on in its understanding of the interplay between data collection as the business model driving big tech, and the impacts that has on us as consumers and as citizens, both from a privacy perspective and from an economic perspective, in terms of Google and Facebook in particular having effective monopolies. Their market worth is entirely based on exploiting our personal information.

FISHER: And what are you hoping for in terms of a final report and legislative consequences? We've seen moves to increase funding of the OAIC and the amount of penalties. What else needs urgently to be addressed?

**JOHNSTON:** Oh my wishlist is long! I would like to see some tightening of the Use and Disclosure principles in Australian privacy law, because too many privacy invasive practices scoot under the radar by saying they are related to the

purpose of data collection. That's a potential outcome of the ACCC enquiry. And I would like to see more public enforcement by the OAIC. Too many cases are declined without a public determination. The State privacy laws are better at allowing individuals to pursue their complaints in a Tribunal, so I would love to see some change there too in relation to the federal Privacy Act. And given the impact of GDPR on Australian businesses, I think Australia should look at beefing up the Privacy Act so that it can be recognised as 'adequate' by the European Union. An 'adequacy' decision would open doors for Australian businesses trying to reach European markets, because then personal information could be exchanged freely.

**FISHER:** CSIRO's Data61 just released a Discussion Paper 'Artificial Intelligence: Australia's Ethics Framework' to encourage conversations about AI ethics in Australia. What were your thoughts about the Government's approach to machine learning and AI technology, from a data governance perspective?

**JOHNSTON:** I have been very critical of the CSIRO's discussion paper. I think that it suffers from a misbelief that privacy law requires consent for everything, but also that getting consent is easy. In the world of AI and ML, consent is actually pretty useless, in terms of a legal ground on which to base your collection, use or disclosure of personal information. Much of the data used to train machine learning will have been collected for some other purpose (like, being a patient in a hospital, or riding a bus), so typically the data subjects were not asked to consent to the use of their data for a different purpose (training a computer to recognise patterns of behaviour). And even if we are to be asked for our consent, how can we possibly give an informed consent, when the whole point of ML and AI is to throw all the data in the mix and see what pops out? They don't necessarily start with a hypothesis for testing. It's not like say a clinical trial, where I know I am being offered a new kind of medicine to treat my disease, and I've been informed about the possible side effects, and I've had the chance to say 'no thanks'. AI and ML are based on different kinds of research practices, which don't usually involve that kind of one-on-one, structured discussion with an individual, or a clearly defined and time-limited purpose for using the data.

So it really concerned me that the government didn't get the basics of privacy law right in this discussion paper. Also, it didn't really get into the ethical dimensions in detail, or questions about social licence. I actually organised a loose coalition of privacy experts to prepare a joint submission to the CSIRO and the Department of Industry (see https://www.salingerprivacy.com.au/2019/04/27/ai-ethics/), because I was so worried that their discussion paper would lull businesses in the tech space into a false sense of security about what they needed to do, in order to comply with privacy law. Risk management in terms of privacy compliance doesn't start or end with getting consent, even if it were feasible in the first place.

**FISHER:** Some scholars suggest that law needs to work in tandem with technology to regulate undesirable uses of technology. For example, you can prohibit spam legally but you can also devise a technological solution – a filter, for example – to prevent or minimise the adverse consequences of undesirable uses of technology. Do you hold high hopes for the prospect of law being able to protect privacy in the digital age? And what are some of the best technological solutions you have seen?

**JOHNSTON:** The law can only ever achieve so much on its own. If tech is designed to allow or encourage users to do things they shouldn't, whether in order to protect their own privacy or that of others, then of course the law and regulators should step in. But it's so much better to bake privacy controls into the design of systems from the beginning. A lot of effort goes into the cybersecurity side of things, keeping out the external bad actors. But when designing, configuring or implementing tech, you also have to think about the authorised users of your system, and design the tech so that authorised users only see the minimum amount of personal information they need to do their job. Saying "oh but we've got a Code of Conduct for our employees" is not nearly enough. The legislation says it's not enough, and case law backs that up. Privacy controls can be built into tech, whether that is filtering out certain data fields from entering a data warehouse, setting role-based access controls on a CRM, masking certain data fields from view of certain users, requiring users to pass certain tests before they can access data (like entering which customer case file they are working on to justify this particular search), audit trials and proactive monitoring of them, just-in-time collection notices or permission requests ... there's plenty you can do. We use eight privacy design strategies to guide our advice to clients when we do Privacy Impact Assessments.

But sometimes the things that stick or that change user behaviour are not high tech at all. I had a client who enforced their policy of staff logging out when leaving their desks in a really novel way. If anyone saw a desktop unattended, they would send an all staff email from that person's email account, saying 'Friday night drinks are on me!' Apparently that changed staff behaviour pretty quickly.

**FISHER:** Nice tip! Anna, thanks so much for this. It's a pleasure as always to get your thoughts about these issues. I know the entire readership is grateful for your insights.

**JOHNSTON:** You're very welcome Eli.

# **Uncharted Waters:** Storm on the Horizon for Online Pirates

**Robert Todd, Paul Dimitriadis and Lachlan Wright,** Ashurst, **report on amendments to section 115A of the *Copyright Act 1968* (Cth), which have given courts new and improved powers to require internet service providers and search engines to block access to websites and other online locations that infringe copyright.**

It would hardly be an article about Australia's website blocking laws without a pirate pun or two.

This *Arrrr*...ticle is no exception.

**Avast ye pirates: A win for copyright owners**

In a move that has been hailed as a win for copyright owners, the *Copyright Act 1968* (Cth) (the Act) has been amended to expand the powers given to courts to deal with the scourge of online piracy by numerous copyright infringers overseas.

The amendments, which were passed with bipartisan support under the *Amendment (Online Infringement) Bill 2018*, and which came into force on 10 December 2018, considerably amended the scope and application of the measures provided for by section 115A of the Act, including by:

- introducing a rebuttable presumption that the website or online location that is the subject of a proceeding brought pursuant to section 115A is located outside of Australia (thereby reducing the evidentiary burden on copyright owners);[1]
- altering the threshold for the grant of injunctive relief to ensure the legislation's applicability to online locations that are shown to have the "primary effect" (and not just the "primary purpose") of infringing or facilitating the infringement of copyright in Australia or elsewhere;[2]
- enabling copyright owners to seek injunctions requiring online search engine providers (other than those that are exempted) to take such steps as the court considers reasonable to remove search results that refer users to impugned websites or other online locations; and[3]
- clarifying that injunctions may be the subject of flexible conditions, to allow copyright owners to block additional domain names, URLs and IP addresses without the parties having to attend court.[4]

As with the previous regime, section 115A provides that Carriage Service Providers (CSPs) and Search Engine Providers (SEPs) are not liable for any costs in relation to court proceedings unless they enter an appearance (for example, to resist the grant of injunctive relief).

## A treasure trove of amendments: What's new?

### Reducing the burden

The amendments significantly reduce the burden on copyright owners who wish to bring an action against the operator of an allegedly infringing website or other online location by introducing a rebuttable presumption that the online location is based overseas. The amendment addresses a key criticism of the previous version of section 115A, which required rights holders to undertake the complex exercise of proving the location of infringing online locations that may employ proxy servers and other techniques to disguise their geo-location.

1 *Copyright Act 1968* (Cth) s 115A(5A).
2 Ibid s 115A(1)(b).
3 Ibid s 115A(2).
4 Ibid s 115A(7).

| Feature of Legislation | Old s 115A | New s 115A |
|---|---|---|
| **Online Location** | Applicant was required to establish that the website or online location was located outside of Australia. | Applicant entitled to rely upon a rebuttable presumption that the website or online location is located outside of Australia. |
| **Test for infringement** | The injunction regime applied to websites and other online locations that were shown to have the "*primary purpose*" of infringing, or facilitating the infringement of copyright. | The injunction regime applies to websites and other online locations that can be shown to have either the "*primary purpose*" or "*primary effect*" of infringing, or facilitating the infringement of copyright. |
| **Scope of respondents** | The court was limited to requiring only CSPs (such as ISPs) to take action against infringing websites by way of injunction. | The court can also require search engine providers (SEPs) to take such steps as the court considers reasonable to remove search results that refer users to impugned websites or other online locations. |
| **Scope of Court orders** | No provision for flexible injunctions. New websites or online locations that the parties became aware of after the proceedings could only be added to the orders for injunctive relief by a court (assuming no agreement was reached out of court). | Injunctions may be the subject of flexible conditions, to allow copyright owners to block additional domain names, URLs and IP addresses without the parties having to attend court to amend the relevant orders. |

The effect of this amendment was recently illustrated in *Australasian Performing Right Association Ltd v Telstra Corporation Limited* [2019] FCA 751 (*APRA v Telstra*), where APRA did not have to establish that the relevant online locations were located outside of Australia, because there was no evidence led to the contrary.

**Primary effect test**

The amendments also broaden the scope and application of the injunction regime to ensure that websites and other online locations that can be shown to have the "primary effect" of infringing, or facilitating the infringement of copyright, may be dealt with. This is significant because under the previous scheme some overseas online locations that facilitated large scale infringement, such as file-hosting websites, could avoid being ensnared by an injunction because it was difficult to establish the "primary purpose" of the website (including, for example, because of the difficulties inherent in proving the intention of the website operator or users of that website).

The new threshold test will ensure that a broader range of overseas websites and file-hosting services (such as cyber-lockers) fall within the scope of the section such that action can be taken to protect rights holders.

The increase and scope was recently illustrated in *Roadshow Films Pty Limited v Telstra Corporation Limited* [2019] FCA 885 (*Roadshow v Telstra*), where an operator of a target online location attempted to argue that his website did not infringe or facilitate the infringement of copyright because his website did not host copyrighted material and only provides indexed and catalogued links to third party websites. Nicholas J quickly dispensed of this argument, finding that the primary purpose and effect of the website was to facilitate copyright infringement.

Despite the increase in scope, it is intended that websites that are operated for a legitimate purpose, but which might contain a small percentage of infringing content, will not be ensnared by the revised regime. However, despite *APRA v Telstra* and *Roadshow v Telstra* being the first two cases decided since the amendments, it still remains to be seen how the "primary effect" test will be applied in practice to more ambiguous websites.

**Search engine providers (SEPs)**

The amendments have significant ramifications for search engines given that the amendments allow a court to require a SEP to take such steps as the court considers reasonable to, for example, remove, demote or disable search results for sites that refer users to online locations blocked under the scheme.

Previously the court was limited to requiring only carriage service providers (such as ISPs) to take action against infringing websites through the injunction regime. However this limitation was widely criticised given that search engine search results leading to various infringing websites often remained live and were available to be clicked on and used by Australian users.

In the ordinary course, the regime will be applied to large search engine providers operating in Australia, including Google, Yahoo! and Bing. However, under the amendments, the relevant Minister has the power to declare, by legislative instrument, that particular online SEPs, or classes of online SEPs, be exempt from the scheme, including smaller operators, such as entities that offer internal (intranet) search functions and entities that provide search functionality that is limited to their own sites or to particular content or material (such as real estate, employment websites or library databases).

**Flexible injunctions**

To prevent the operators of overseas websites (and other online locations) from circumventing injunction orders by using a different domain name or creating a different URL for the purpose of providing a pathway to infringing content, the court is empowered to grant injunctions that have flexible terms and conditions. According to section 115A(2B), such injunctions can apply to domain names, URLs and IP addresses that come into existence after an injunction is granted provided that the parties agree to add those additional pathways to the terms of the injunction.

The flexibility has been enshrined in the amendments for the purpose of resolving any ambiguity with respect to the previous injunction regime and comes with the added benefit of saving the parties and the court the time and expense of having to return to court to amend injunction orders.

For the avoidance of any doubt, the Explanatory Memorandum to the *Amendment (Online Infringement) Bill 2018* specifies that any injunctions issued by a court are limited in application to Australia, meaning that a court cannot, for example, require a SEP to block search results worldwide.

## Navigating uncharted waters: The way forward

Proponents of the amendments claim they improve the adaptability and responsiveness of the relevant provisions of the Act.

The amendments are also in line with steps taken by regulators in other jurisdictions to place greater responsibility upon SEPs and other intermediaries for copyright infringement, a trend that is expected to continue (see for example, the EU Directive on Copyright in the Digital Single Market).

However, given the cost and expense of prosecuting proceedings for an injunction, the regime provided for under section 115A may ultimately only be engaged with as a last resort. Provided that the relevant parties reach agreement on which sites to block, and the impugned website or overseas location does not resist the measure, a section 115A injunction is moot.

In the ordinary course, copyright owners that wish to avail themselves of the mechanisms under section 115A should seek advice and engage in correspondence with relevant stakeholders as early as possible. It may be that a commercial outcome can be reached cost effectively through negotiation and without the need to prosecute an injunction against a pirate.

# CAMLA Young Lawyers Networking Panel Event

**By CAMLA Young Lawyer Committee representative Madeleine James. Photos: Amy Campbell**

On 3 June, the CAMLA Young Lawyers Committee held their annual Networking Event, hosted at the offices MinterEllison.

Attendees at the sold-out event heard from an esteemed panel about career development as well as approaches to networking and participated in interactive app-based sharing of networking experiences, before connecting with other professionals over drinks.

The CAMLA Young Lawyers again thank panellists Ben Cividin (Head of HR, Kayo Sports), Ben Kay (Partner, Kay & Hughes, Art and Entertainment Lawyers), Nick Pascoe (Partner, MinterEllison), Sophie Malloch (Associate General Counsel, Facebook Australia and New Zealand) and Rebecca Sandel (Senior Director, Legal & Business Affairs, Universal Music Australia), for participating in the event.

The audience heard from the panellists about their personal experiences and views on networking, and gained valuable insights such as:

- Be genuine with all interactions, including on social media – insincere and constant LinkedIn posts are easy to spot and can be quite off-putting.
- Do your research, and don't be afraid to reach out to someone working in the field or job of your dreams to learn about how they got there. Most people will respond to genuine enthusiasm.
- Networking is all about playing the long game. It might be years before a job opens up, but if you've made an impression in the past, it can help to set you apart from other applicants.

Eli Fisher (HWL Ebsworth) and Ashleigh Fehrenbach (MinterEllison), editors of the Communications Law Bulletin, announced the winners of the CAMLA Essay Competition:

1. Cheng Vuong "Defamation Law and the Search Engine Exception"
2. Nathan Saad "Platform liability for its user-generated content"
3. Ryan Piezsko "Suppressing Information in the Information Age"

The evening was moderated by Katherine Sessions (Chair of the CAMLA Young Lawyers Committee, Office of the eSafety Commissioner), with assistance throughout from CAMLA Young Lawyers Amy Campbell (HWL Ebsworth), Calli Tsipidis (Fox Sports), Marie Karykis (Foxtel) and Joel Parsons (Bird & Bird).

Thank you again to our terrific panellists and MinterEllison for generously hosting the evening. We look forward to seeing you at our next CAMLA Young Lawyers Networking Event in 2020.



# **Hells Angels Hath No Fury:** An Insight Into Internet Intermediaries

**Laksha Prasad, Graduate, HWL Ebsworth, considers the Hells Angels claim against Redbubble.**

Earlier this year, the Federal Court of Australia ruled on a copyright and trade mark infringement claim brought by the local chapter of the Hells Angels motorcycle club (HAA), against online marketplace Redbubble.

The allegations, which concerned Redbubble's use of the club's name and notorious 'death head' trade mark (as well as its derivative, the 'Fuki' death head), touched on the liability of internet intermediaries for infringements perpetrated by their users.

The Melbourne-based marketplace provides a platform for users to upload their creative works to the Redbubble website so that customers can select and order prints of the works on a range of paraphernalia, including t-shirts and phone cases. However, the infamous bikie club found that a number of their registered trade marks were being uploaded by Redbubble users, printed onto merchandise and sold without their permission.

As a result, HAA claimed that Redbubble either directly infringed HAA's copyright by communicating HAA copyright works to the public, or that Redbubble was jointly liable with its users for authorising the upload of the works and trade marks onto the Redbubble website.

Redbubble refuted the allegation by stating that it only acts as an agent for its users by enabling a transaction to occur between independent users and buyers operating within its marketplace. Further, Redbubble argued that any infringing conduct was beyond the jurisdiction of Australia IP law since its servers were located in the United States. Nonetheless, Redbubble removed the offending material from its site (which did not stop HAA from demanding compensation for the money Redbubble made from selling the items) and entered a cross-claim on the basis of non-use of registered trade marks owned by Hells Angels' US-based parent company.

In its consideration of HAA's copyright claim, the Court considered the subsistence of copyright in the 'death head' membership card image and the 'Fuki' death head design.

While HAA asserted that they were 'granted' an exclusive licence in the copyright works for use in Australia by the club's American headquarters (HAMC US) - it was held that Redbubble did not infringe HAA's copyright since it could not be established that HAMC US was the original copyright owner of the works (which would have otherwise seen Redbubble deemed as a primary infringer of HAA's copyright) and therefore could not grant a licence to HAA. Similarly, copyright was not found to have subsisted separately in the 'Fuki' design since it was a derivative work of the membership card and no effort, skill or work was exercised by the artist when producing the work.

The question of trade mark use, however, appeared to have a more favourable outcome for the bikie club. The court examined Redbubble's business model and deemed that Redbubble had exercised sufficient management, control and power over the chain of supply of the relevant goods to conclude that three of the four HAMC US-owned trade marks had been infringed. Specifically, the court was satisfied that Redbubble had 'used' the relevant trade marks in Australia as a 'badge of origin' - resulting in the award of $5000 in damages for the use of the marks owned by HAMC US.

Redbubble's cross-claim also failed on the basis that HAA was able sufficiently to establish itself for which the relevant trade marks were registered. Accordingly, the Court refused to exercise its discretion to remove the marks from the register.

The trade mark left out of the infringing pile - an image of a child with a demon (together a 'hells angel') - was not considered to have constituted a 'use' of a HAA trade mark since it was seen as a mere parodic composition.

The HAA decision is comparable to the earlier *Pokémon v Redbubble* case, which saw the notable Japanese franchise commence proceedings against the online marketplace over merchandise that bore approximately 29 of the 800 Pokémon characters and associated logos of them on the Redbubble website.

Of particular note was the use of the most recognisable Pokémon character Pikachu, which sparked allegations that Redbubble had infringed sections 18(1), 29(g) and (h) of the Australian Consumer Law. The Court ultimately held that the use of Pokémon's images misled consumers as to the authenticity of the merchandise sold on the website and, as such, Redbubble had made representations that the relevant 'works' supplied on their site were authorised by Pokémon.

Pagone J found that copyright subsisted in the 'artistic works' hosted on Redbubble's website and

that Pokémon was the owner of such copyright on the basis of its United States copyright registration certificate; and that Redbubble infringed Pokémon's copyright by communicating Pokémon images to the public by offering/exposing/exhibiting the works by way of trade through the Redbubble website and authorising reproduction of the works in Australia.

Notwithstanding Pokémon's success on these points, the Court only awarded Pokémon $1 in nominal damages (and 70% of their court costs) to be paid by Redbubble, on the basis that most of the infringing items were 'mash-ups' that would not entitle Pokémon to royalties, and no loss or damage had actually been suffered.

In both cases, the Court took note of the inherent commercial risks of Redbubble's business model, namely the prospect of an online marketplace without an adequate intellectual property policy. That's not to say that Redbubble didn't have any in place - it had some form of intellectual property policy and a team dedicated to ensuring advertised products were compliant with copyright law, both of which were crucial to the Courts' ruling that the infringements weren't 'flagrant' in nature. Nevertheless, such a business did pose inherent risks.

Given the lack of significant penalties being awarded in respect of Redbubble's conduct, the Court highlighted how other internet intermediaries may seek to follow Redbubble's lead in employing bare takedown procedures and IP policies as a means to mitigate any future IP infringement claims.

However, the Court also rejected Redbubble's defence in the HAA case, namely that it acts as an agent in the transactions entered into by the artists and the artists' customers. Instead, the Court considered the nature of internet intermediaries to go beyond an agent-principal relationship. Rather, given the amount of autonomy such online marketplaces exercise in hosting, sponsoring and arranging certain products on their websites, such sites play a role more reflective of an 'independent contractor' in such transactions - which will always expose them to some level of liability.

# **Objective Failure:** Defamation Law Reform and the Lack of Regard to the Objects of the Defamation Act

**By Robert Todd, Partner and Rachel Baker, Lawyer at Ashurst**

Submissions to the Council of Attorney's-General Review of Model Defamation Provisions (MDP, the Review) have closed, and among the 33 responses[1] from practitioners, interest groups and publishers a degree of consensus can be discerned that some areas of defamation law are in need of reform, specifically jurisdictional discrepancies, qualified privilege, contextual truth, single publication and innocent dissemination. These areas of agreement among the submissions reflect a widely held view that the application of defamation law in Australia has had insufficient regard to the stated objects and structure of the Uniform Acts.[2]

These objects are:

(a) to enact provisions to promote uniform laws of defamation in Australia;

(b) to ensure that the law of defamation does not place unreasonable limits on freedom of expression and, in particular, on the publication and discussion of matters of public interest and importance;

(c) to provide effective and fair rem-edies for persons whose reputations are harmed by the publication of defamatory matter; and

(d) to promote speedy and non-litigious methods of resolving disputes about the publication of defamatory matter.

The structure of the Uniform Acts was intended to support these objects by, amongst other means:

1. Introducing a regime to encourage early settlement offers (Offers of Amends);
2. Removing the rights of corporations to sue;
3. Discouraging a multiplicity of actions;
4. Promoting settlement by capping damages, and creating more certainty as to damages outcomes;
5. Discouraging forum shopping caused by differential approaches across Australian jurisdictions; and
6. Engaging community standards and participation in the adjudication of matters of public interest and importance.

Many of the drafting issues that have recently arisen were addressed by media interests in the lead up to the enactment of the Uniform Acts, which led to the inclusion of section 49, providing for a review of the operation of the legislation.

While judgments in defamation matters frequently refer to these objects, it is arguable that, based on various lines of authority, insufficient weight is given to them in decision-making. It is also the case that the objects are rarely referred to in cases involving publication of a matter claimed by the defendant to be in the public interest, where a defence of qualified privilege is raised.[3]

Concerns about the punitive action of defamation law on news reporting are echoed by the Alliance for Journalists' Freedom which, shortly after the closure of submissions to the Review, released a White Paper, titled Press Freedom in Australia (the White Paper). The White Paper argues that legal developments have "chipped away at the fundamental freedoms and protections that allow journalists to do their important work".[4] It calls for a Media Freedom Act to reform legislation affecting news reporting and the introduction of a clearly set out public interest defence for defamation (discussed below under Qualified Privilege).

## Object (a): uniform laws of defamation in Australia

Since the decision in *Crosby v Kelly* [2012] FCAFC 96, the door has been opened for the Federal Court to exercise jurisdiction over "pure" defamation matters. By relying on section 9(3) of the *Jurisdiction of Courts (Cross Vesting) Act* 1987 (Cth) the Federal Court concluded that it had the jurisdiction to hear and determine those matters which were within the jurisdiction of the ACT Supreme Court. Since *Crosby* and subsequently *Hockey v Fairfax*[5], the Federal Court has held that the publication in a territory (amongst other places) provided the Federal Court with jurisdiction to hear the matter.[6]

The consequence of these events is that plaintiffs can commence defamation proceedings in the

1 As at 3 June 2019.
2 In this article, references to sections are references to the *Defamation Act 2005* (NSW).
3 For example, *Hockey v Fairfax* (2015) 332 ALR 257; *Cummings v Fairfax* [2018] NSWCA 325; *Chau v Fairfax Media Publications Pty Ltd* [2019] FCA 185
4 Alliance for Journalists' Freedom, Press Freedom in Australia, 2019
5 [2015] FCA 652.
6 Communications Law Bulletin, Vol 37.4 (December 2018) page 3.

Federal Court and avoid a trial by jury. Because of the contradiction between section 39 of the *Federal Court Act 1976* (Cth) (which provides that civil trials shall be heard by a Judge alone, unless the court orders otherwise) and section 21 of the MDP (which section is enacted in all states except South Australia, the ACT and Northern Territory, and which provides that either party can elect for a trial by jury, unless the court orders otherwise) there is now a significant discrepancy in defamation laws between jurisdictions. This is the case because, under the Constitution, Commonwealth legislation prevails over state legislation to the extent of any inconsistency.

Trial by jury was seen to have a significant role in advancing the objects of the Act by bringing community expectations and interests directly to bear on the issues in dispute. It also imposed a degree of practical rigour on the management of trials. The outlier State and Territories excluded juries for historical reasons.

The unforeseen and rapid evolution of the Federal Court's jurisdiction has led to forum-shopping by plaintiff lawyers. It has also created a discrepancy that undermines object (a) of promoting uniformity, and also object (b) of avoiding unreasonable limits on freedom of expression, because it undermines the choice provided by section 21 of the MDP. Several submissions to the Review argue that jurors provide a better reflection than a judge alone of the "ordinary reasonable reader" relied upon in defamation law. David Rolph argues:

> "The issue of defamatory meaning is fundamentally a matter of impression, to be assessed by reference to the standard of the ordinary, reasonable reader or listener or viewer, who is a layperson and not a lawyer. Juries are able to reflect this standard more closely than judges and are more representative of the community than judges. Given the interests involved in defamation – the protection of reputation and freedom of speech – interests in which every person has a stake – ordinary people sitting on juries should continue to play a role in defamation cases."

Defamation is a tort in which the public has a very direct interest and therefore the involvement of the public as jurors engages the community in the administration of justice in an area of law that affects the general public. If the public is excluded by reducing the role of juries, there is a significant risk that the Courts will be seen to be out of touch with community standards. Judges often assert that jury trials are a burden on the system but, in the experience of practitioners, the opposite can be the case: lawyers running a trial before a jury are compelled to be more precise and efficient.

Australia's Right to Know Coalition (ARTK, representing mainstream mass media publishers) suggests the following measures to remove the discrepancy:

a) The Federal Government become a signatory to the Intergovernmental Agreement for the MDP;

b) The Federal Government amend the *Federal Court of Australia Act 1976* (Cth) to incorporate sections 21 and 22 of the MDP; and

c) The ACT, South Australian and Northern Territory laws also be amended to incorporate sections 21 and 22 of the MDP.

Rolph also suggests the Defamation Working Party (DWP) give "detailed consideration" to the broader ramifications of the Federal Court's jurisdiction over pure defamation claims. The Chief Justice of South Australia, though, opposes the introduction of jury trials in that state. Chris Kourakis argues that determination of defamation matters by judge-alone is "more efficient, more just and results in fewer appeals".

## Object (b): avoiding unreasonable limits on freedom of expression and, in particular, on matters of public interest and importance

The application of the Uniform Acts by the Courts has had the practical effect that, absent a successful plea of truth, the media has no defensible opportunity to bring matters of public importance and interest to the attention of the public. The structural objectives of the Act have been severely undermined.

### Qualified privilege

Most respondents submit that the failure of statutory qualified privilege to protect public interest journalism is a significant problem. The unrealistic standard of reasonableness imposed on the media is leading to judgments going against publishers for cases involving what could be characterised as quality investigative journalism, albeit containing some elements found to be untrue, such as *Fairfax v Obeid*[7] and *Chau v Fairfax*[8]. Judgments in defamation cases often do not acknowledge that news media will, despite the best practices and most thorough research, sometimes publish statements that turn out to be false, or at least cannot be proven true to a judicial standard. This can be the case because sources provide information about matters of public interest on the condition of anonymity (and those sources cannot then be called as witnesses), sources may provide information that turns out to be false, or journalists can, acting honestly and ethically, make mistakes. As ARTK points out, in such cases "it is considered better that they speak out and get it wrong, than say nothing at all." Patrick George argues

7 [2003] NSWSC 967.
8 [2019] FCA 185.

that the rise of new media makes the need for reform more pressing:

> "It is in the public interest in these times of manipulation of the news and reputations by use of social media and the internet that a professional journalist can report with a margin of error, but with due care having regard to the fragile nature of reputation and the risk that reputations can be easily destroyed."[9]

The fact that statutory qualified privilege has not been successfully used by any media defendant since the MDP were enacted highlights that either the defence needs to be reformed, or a separate defence for mass publications on matters of public interest should be introduced, similar to section 4 of the *Defamation Act 2013* (UK). The latter view is supported by the White Paper, which argues that the need for such a defence is demonstrated by the inaccessibility of qualified privilege, and the High Court's refusal to hear a number of cases that have sought to explain or expand defences that may be available based on the constitutional implied freedom of political communication.

Rolph however warns that the introduction of a public interest defence may be ineffective because, unlike courts in the United Kingdom and other Commonwealth countries, Australian courts have not recognised a common law defence of publication to the world at large on matters of public interest. Because there would necessarily be a degree of judicial latitude in determining whether a matter was truly in the public interest and whether the publisher reasonably believed it was so, Rolph argues there is a risk such a defence could turn out to be as unreliable as the current qualified privilege provision. The alternative, of waiting for the common law to recognise such a defence, may be unpalatable to many stakeholders. The situation could be assisted by ensuring greater involvement of juries in assessing the reasonableness of publishers' conduct, which would involve amending the *Federal Court of Australia Act 1976* (Cth) (as discussed above) to allow for the election of juries to decide defamatory meaning and questions of fact relating to defences.

### Contextual truth

Another defence that seeks to counterbalance the chilling effect of defamation law is contextual truth, but this too has proven inaccessible for media defendants. The cause of the problem appears to lie in the drafting of clause 26 of the MDP, where the words "in addition to" have been included, preventing the practice of defendants pleading back the plaintiff's imputations. The result is that, where a plaintiff pleads a range of imputations, and the defendant can prove the truth of only some of them, the defendant cannot rely on the true imputations to argue that the plaintiff's reputation has not been further harmed by the imputations whose truth it cannot prove. Further, since *Besser v Kermode*[10], NSW courts have held (although not always)[11] that a plaintiff can amend its defence to adopt imputations pleaded by the defendant for the purposes of contextual truth, thus depriving the defendant of their defence (because the defendant's imputations will no longer be "in addition to" the plaintiff's).

Most submissions to the Review, including the Law Council of Australia, the NSW Bar Association, the Bar Association of Queensland, ARTK, Rolph and Dr Daniel Joyce of UNSW Law, argue that this clause should be redrafted to more closely reflect its predecessor in the 1974 Act. Nearly a decade ago, this problem was highlighted by Simpson J[12] but it has not been remedied. The submission by Leanne Norman et al[13] suggests the drafting was an unintended error that could be avoided in the future by appointing a panel of experienced specialist defamation practitioners to oversee the drafting process.

### Single publication

The submissions reflect general agreement that the multiple publication rule should be abolished in favour of a single publication rule with a 12 month limitation period. The multiple publication rule is based on a principle established by an English court in 1849[14] and is unsuited to the digital era, where each download of an article is regarded as a separate publication, at which point the limitation period recommences.

The rule was confirmed by the High Court as applying to internet publications in *Dow Jones v Gutnick* [2002][15]. Digital industry group DIGI has submitted to the Review that this decision was based on an internet described by their Honours as a medium no different to radio and television, which their Honours doubted could be described as having a "uniquely broad reach".[16] DIGI argues that, even if those statements were true then, they are not true now. In the intervening 17 years the internet has become more pervasive and publication more instantaneous, such that the internet is dramatically different to the forms

9 Patrick George submission, page 10.
10 *Kermode v Fairfax Media Publications Pty Ltd* [2010] NSWSC 852, [56]
11 *Dominello v Harbour Radio Pty Limited t/as 2GB* [2019] NSWSC 403.
12 *Kermode v Fairfax* [2010] NSWSC 852, [56]
13 and Bruce Burke and Phillip Beattie of Banki Haddock Fiora.
14 *Duke of Brunswick v Harmer* (1849) 14 QBD 185
15 194 ALR 433; 77 ALJR 255 (10 December 2002)
16 Ibid [39]

of publication that have existed in the past.

As well as creating ongoing liability for publishers, the multiple publication rule can create issues for other defences, as highlighted by DIGI. In *Google v Duffy* [2017] SASCFC 130, Peek J held that Google could only rely on the qualified privilege defence if it could prove that it had acted reasonably in relation to each of the "publications" of the search results in question. The plaintiff had not identified the recipient of each publication, but it was held that Google had to identify each individual and enter evidence about the circumstances of their search for and receipt of Google snippets.

**Innocent dissemination**

This section of the Review attracted the only submission from outside Australia, from Stanford University's Center for Internet Studies. The Center runs an Intermediary Liability project, which proceeds from the position that holding internet platforms liable for their users' online activity is a form of "censorship-by-proxy" and a restriction on free speech and innovation. The Center points to a joint declaration of international mandate holders on freedom of expression, "fake news", disinformation and propaganda, made on 3 May 2017, which stated:

> "Intermediaries should never be liable for any third party content relating to those services unless they specifically intervene in that content or refuse to obey an order adopted in accordance with due process guarantees by an independent, impartial, authoritative oversight body (such as a court) to remove it and they have the technical capacity to do that."

The Center argues that the reasoning used in *Google Inc. v Duffy*[17], that Google's liability as a secondary publisher was based on its intentional design of its search engine to produce results in the way it did, its facilitation of the reading of the defamatory material in an indispensable, substantial and proximate way, and the fact it had received notice and had a reasonable timeframe to block the offending content, highlights the need for reform. It submits that for the purposes of the innocent dissemination defence internet intermediaries should be automatically considered subordinate distributors in any case.

It is clear that communication technologies have evolved beyond the intended scope of the innocent dissemination defence, as drafted in section 32 of the MDP. DIGI, ARTK and Google submit that the MDP should be amended to encourage claimants to pursue original authors of offending content, rather than distributors. DIGI and ARTK argue that the notion of "editorial control" in section 32 is outdated in the digital context and should be removed or revised.

The internet involves the distribution of billions of pages of content every day, without human supervision. The Law Council of Australia and Norman et al point out that the net effect of the current innocent dissemination defence in the MDP is that internet hosts are in a better position in terms of legal liability if they do not take steps to monitor content they host. Furthermore, if hosts do monitor content or receive a complaint about allegedly defamatory material, the legislation does not allow for regard to defences such as truth or privilege. The result is that this defence has the potential to allow a chilling of free speech because the only way a defendant can rely on it is to block or hide content that is prima facie defamatory or about which a complaint is received.

The Bar Association agrees that innocent dissemination is an area in need of reform, but submits that the problems associated with digital publishers should be dealt with Federally. Furthermore, they agree that reform should also address issues including intellectual property infringement, vilification and hate speech and dissemination of terrorism material.

Many submissions support the idea of digital platforms being afforded a safe harbour from liability for third party content. Google and DIGI argue it is inappropriate for them to be arbiters of defamatory content and defences (which is the consequence of holding them liable for not removing material following a complaint). University of Western Australia Law School's Michael Douglas argues that a safe harbour is in the interests of justice, because "to outsource the judicial function to a for-profit multinational should be approached with hostility by all those who appreciate the rule of law". University of Technology Sydney's Centre for Media Transition submits that excluding digital platforms from the definition of publisher does not absolve them of legal responsibilities, it just means their responsibilities are different to those of publishers.

## Objects (c) and (d): effective and fair remedies; speedy and non-litigious resolution of disputes

Addressing the concerns above would also significantly advance the third and fourth objects of the MPD:

(c) to provide effective and fair remedies for persons whose reputations are harmed by the publication of defamatory matter; and

(d) to promote speedy and non-litigious methods of resolving disputes about the publication of defamatory matter.

By improving defences so they operate as intended and deal with public interest journalism more fairly, and by focussing disputes

17 [2017] SASCFC 130.

between complainant and originator (rather than distributor) remedies will be fairer and more effective. The resolution of disputes will also be faster and more efficient, because it will reduce resources being expended on vexed questions of publication and reasonableness.

Section 35 provides that there is a cap on damages for non-economic loss. The practice of Courts exceeding that cap where aggravated damages are awarded undermines objects (c) and (d) because the cap is intended to promote certainty and encourage the settlement of disputes without resort to litigation. Consistency in damages is important to non-judicial resolution of disputes, and was recognised by the Court in *Cerutti v Crestside Pty Ltd* [2014] QCA 33 at 54:

> "...principles of compensation, the statutory command in s 34 of the Act to ensure "an appropriate and rational relationship" with the harm sustained and the need for some consistency between closely comparable cases constrain the proper exercise of discretion. Some level of consistency in awards is important to enable parties to predict with some confidence what an award is likely to be at trial, and to resolve their differences based on that prediction."

## The path to world's best practice

Australia's defamation laws are more plaintiff friendly than those of comparative jurisdictions, such as the United Kingdom, United States Canada and New Zealand. While the states of Australia inherited the common law of England, (and each then proceeded to reform it disparately until the enactment of the Uniform Acts in 2005) it is not clear why it the laws of Australia took such a pro-plaintiff path, compared to other Commonwealth countries.

For a nation whose culture has been so shaped by an appreciation for frankness and a willingness to criticise others (to the extent that we even have a name for criticising successful figures in "tall poppy syndrome") it is not clear why those values have not been so influential when it comes to defamation law.

Whatever the reasons for the current state of affairs, it is apparent that the situation is unfortunate and deserving of attention from legislators. As the NSW Bar Association implored in its submission:

"It is imperative that Australia, let alone NSW, is both seen to have, and does have, a modern and consistently applied law of defamation which at the very least meets the world's best practice in the defamation community and embraces, and is underpinned by, contemporary thoughts."

It is clear that, at a minimum, in order to be faithful to the original statutory intention the Review should carry out the following:

1. Address forum shopping and involve the public in the adjudication of maters;
2. Provide for a workable defence of qualified privilege;
3. Amend the general damages provisions to ensure damages are not, in certain circumstances, at large so as to promote the settlement of disputes;
4. Introduce a single publication rule;
5. Amend the defence of contextual truth; and
6. Adopt section 1 of the UK Act to provide that only serious defamatory matter is actionable.

# 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)