CAMLA COMMUNICATIONS LAW
BULLETIN
Communications & Media Law Association Incorporated
Volume 39, No 1. April 2020
New Decade Edition

# Copyright in the 2010s
## The Decisions that Defined the Decade

**Rebecca Dunn,** partner, and **Natalie Zwar** and **Caitlin Meade,** lawyers, Gilbert + Tobin, discuss the evolution of copyright law in the 2010s and where copyright law is headed in this new decade.

### Introduction

If the first decade of this century established and began to test new copyrights for the digital age, the second explored the scope and limits of the operation of those rights in the online environment.

In the 2000s we saw the introduction of the communication right and the codification of the law of authorisation (*Digital Agenda Act*[1]), the first tests of enforcement of the communication right and the authorisation of infringements of that right (*Cooper*[2] and *Kazaa*[3]), consideration of the way copyright law can apply to the internet environment via hyperlinking and P2P (*Cooper* and *Kazaa*) and the way copyright subsistence and originality apply to digitally generated content (*IceTV*[4]).

In the 2010s each of those issues was further explored, with the Courts considering the limits of the operation of copyright law as it interacts with online business models and realities. In 2010 in particular there were multiple important copyright judgments, many of which went on to be appealed to higher courts. These cases form the framework for the development of copyright law in the digital environment in the last decade and provide guidance as we enter the next.

Meanwhile, as the Courts grappled with the application of new technologies to the law, there were numerous enquiries into whether legislative amendments should be made to the *Copyright Act 1968* (Cth) (the **Act**) to accommodate the impact of those technologies on traditional and new business models. The majority of those enquiries resulted in recommendations which have not been implemented, leaving copyright law in the hands of the Courts for now as we head into the 2020s.

### Case Law

#### Originality

At the close of the 2000s, the High Court of Australia delivered a landmark decision on originality in Part III works, in *IceTV*. The Court delivered two separate judgments, from French CJ, Crennan and Kiefel JJ on the one hand and Gummow, Hayne and Heydon JJ on the other.

1 *Copyright Amendment (Digital Agenda) Act 2000* (Cth).
2 *Universal Music Australia Pty Ltd v Cooper* [2005] FCA 972; *Cooper v Universal Music Australia Pty Ltd* [2006] FCAFC 187 (**Cooper**)
3 *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 222 FCR 465
4 *IceTV Pty Ltd v Nine Network Australia Pty Ltd* [2009] HCA 14 (IceTV).

## Contents



CAMLA

**Editors**
Ashleigh Fehrenbach and Eli Fisher

**Editorial Assistants**
Isabella Street and Claire Roberts

**Design | Printing | Distribution**
MKR Productions

# Editors' Note

Dear readers,

Happy new year, happy new decade, and (most momentously) happy new edition of the CLB!

We hope you are staying safe in these uncertain times.

We are pretty sure that the new decade has already used up its quota of horrible, and it's only March 2020. We hope that you are all keeping safe and sound, and that this edition helps to alleviate the isolation. Worst case, it may help to alleviate the toilet paper shortages.

This will pass. And before too long, we will be back together meeting at seminars and cocktail parties and being whatever the opposite is of socially distant ("antisocially intimate"?).

Speaking of the new decade, this new edition has a special '**new decade**' theme. We have procured for you a range of thought leaders (and also Eli) to discuss the previous decade in relation to a specific body of law, and suggest an agenda for the new decade. For older CAMLA members, this might be a really nice stroll down memory lane as you reflect on a decade's worth of matters on which you worked, judgments you read, and fascinating CAMLA seminars you attended. For younger CAMLA members, this is a really great way to catch up on what was taking place before you joined the scene, and provide some helpful context for the matters you're thinking about and working on today. And if you're reading CLB, you're hopefully self-isolating responsibly and not converging on Bondi Beach.

We have our friends at Gilbert + Tobin, **Bec Dunn, Natalie Zwar and Caitlin Meade**, take us through copyright law. Everyone's favourite **Emma Johnsen**, of Marque Lawyers, walks us through eSports. Telco experts **Joel von Thien and Jono Selby**, from Clayton Utz, discuss telecommunications.

Minters' **Katherine Giles** describes the decade in contempt law, suppression orders and open justice. **Patrick Fair** of Patrick Fair Associates provides an overview of national security law as it relates to technology. **Maddie James and Jim Micallef** from Corrs tell us what's been (not) happening in the privacy tort space over the last decade, and what might yet be to come in the 20s. **Sophie Dawson** and **Phil Gwyn** from Bird & Bird summarise the previous decade in defamation law. And Baker McKenzie's **Eli Fisher** has a look at data privacy law.

But wait, you want more? CAMLA Young Lawyer, **Claire Roberts**, of counsel, profiles **Associate Professor Jason Bosland**, media law expert at Melbourne University to chat about his career and some of his thoughts on defamation and suppression orders across the decades.

CAMLA kept us in touch throughout the 2010s. In touch with the law. In touch with key industry developments. In touch with each other. Our confident prediction for the coming decade, especially these very strange, chaotic, WFH times, is that CAMLA will play an identical - if more important - role.

To that end, check out the ad within for the **webinar** on **Coronavirus, Contracts and Cancellations in the Tech-Media space**, hosted by Baker McKenzie's TMT team on **8 April 2020**. Please don't stockpile tickets. There's enough to go around.

We also report on the magnificent **CAMLA Young Lawyers networking event** at Clayton Utz.

There's a lot going on in our space, and the next edition - shortly to follow - will cover these developments. In the meantime, stay safe and look after each other. (And don't send in angry letters to the editor about whether, technically, the new decade starts on 1 January 2021. We're not interested.)

**Ash and Eli**

The judgments proceeded via very different reasoning but reached the same outcome, reversing the decision of the Full Federal Court and finding in IceTV's favour that its television guides did not infringe Nine's copyright in its own television guides. In doing so, the High Court reset the test for originality, essential for subsistence of copyright and relevant to whether a substantial part of a work has been infringed.

Despite the fact that copyright in the relevant works was admitted by IceTV at trial, each of the judgments of the High Court treated the individual parts of the work as lacking sufficient originality to be protected by copyright. The French decision described such individual parts of the information in relation to a given program as "not a form of expression which requires any particular mental effort"[5] whose arrangement in chronological order was "obvious and prosaic, and plainly lacks the requisite degree of originality"[6]. The Gummow judgment went further finding that final steps in the creation of the relevant works involved "extremely modest skill and labour"[7] even though copyright had been admitted. Additionally, the Gummow judgment in particular took a fresh look at authorship, casting doubt on whether works will be protected by copyright where detailed evidence of authorship cannot be provided, or where the number of authors, or steps involved to identify them, make gathering that evidence impractical or impossible.

### *Phone Directories*

Against the backdrop of the *IceTV* case, one of the earliest copyright judgments delivered in the 2010s was the first instance decision in *Telstra Corporation Limited v Phone Directories Company Pty Ltd* [2010] FCA 44 (the **Phone Directories case**). The case was subsequently appealed to the Full Federal Court and the decision of the trial judge (Justice Gordon) upheld.[8]

5 *IceTV* at [42].
6 *IceTv* at [43].
7 *IceTV* at [168].
8 *Telstra Corporation Limited v Phone Directories Company Pty Ltd* [2010] FCAFC 149 (*Phone Directories Full Federal Court*).

The case concerned the question of whether copyright subsisted in Telstra's White and Yellow Pages telephone directories. Justice Gordon held that copyright did not subsist in the directories as they were not original works capable of protection under the Act. Telstra had not identified many of the authors of the directories, and even if they had been identified, the work done in creating the directories did not constitute "independent intellectual effort" or was not "sufficient effort of a literary nature". Further, the work was done prior to the directories taking material form and was therefore not relevant to the question of originality, and finally and importantly, the work was computer generated, rather than the result of human effort.[9]

On 15 December 2010, the Full Federal Court unanimously upheld Justice Gordon's decision. Applying *IceTV*, the Full Court held that to be original, a work must originate from a human author and be the result of "independent intellectual effort" which is directed to reducing the work to its material form.[10] Telstra argued that its gathering/organising and ordering/arranging of the material contained in the directories constituted independent intellectual effort. The Full Court rejected this, finding that the gathering and ordering phase was not directed to the reduction to material form, and that the ordering and arranging phase was not undertaken by human authors but by a computerised process.[11] The Full Court did agree with Telstra's submission that in proving originality and subsistence, it is not necessary to identify by name each and every author of a work. Rather, it must be demonstrated that the work originated from a human author or authors.[12] In this instance, because of the role of computerised and automated processes, that requirement was not met. The emphasis on human authorship leaves vulnerable computer-generated products and databases into which considerable effort is expended, but no human author can be identified. Whether or not such works should be protected will be a live issue into the next decade.

Telstra applied for special leave to appeal to the High Court, but leave was not granted.

***Fairfax v Reed***

Exploring the issue of originality in aggregated works further was the case of *Fairfax Media Publications Pty Ltd v Reed International Books Australia Pty Ltd* [2010] FCA 984 (**Fairfax v Reed**).

Reed (trading as "LexisNexis") provided a service known as ABIX, through which it provided abstracts of articles (usually comprised of the headline and by-line, together with a summary of the article written by a Reed employee) published in a range of Australian newspapers, including the *Australian Financial Review*. Relevantly, Reed did not publish the full articles. Fairfax filed proceedings against Reed for copyright infringement. The primary issue before the Court was whether or not the pleaded works were original literary works, including individual headlines.

Fairfax selected ten headlines for consideration and filed evidence of the skill and effort invested by sub-editors in their creation, as well as the purpose and value of a headline in "attracting readers to read the articles". Justice Bennett held that the headlines included in the case were not literary works, and found that "headlines generally are, like titles, simply too insubstantial and too short to qualify for copyright protection as literary works".[13] Her Honour noted:[14]

> *There may well be writings of original words or phrases that simply do not reach the level of constituting a "work", regardless of literary merit. This is not just because they are short, as a deal of skill and effort can go into producing, for example, a line of exquisite poetry. It is because, on its face and in the absence of evidence justifying its description as a literary "work", the writing does not, qualitatively or quantitatively, justify that description. A headline is, generally, no more than a combination of common English words (Dicks v Yates at 88 per Jessel MR). It 'does not involve literary composition, and is not sufficiently substantial to justify a claim to protection' (Francis Day at 122-123); it does not, in the words of Jacobson J in Sullivan at [112], have 'the requisite degree of judgment, effort and skill to make it an original literary work in which copyright may subsist' for the purposes of the Act.*

Justice Bennett's decision also continued the pattern started in *IceTV* and developed in the *Phone Directories* case in focusing on the need to define and prove the authorship of copyright works. In relation to the authorship of the headlines, Fairfax was unable to rely on the presumption in s 129(2) of the Act in respect of each of headlines as a basis for establishing their originality[15] because the unidentified team of sub-editors who authored the headlines in question were in Fairfax's employ and the requisite enquiries to establish their identifies had not been made.[16]

This issue also informed the separate question before the Court as to whether the combination of an article, its headline and associated by-line could also be considered a discrete original literary work. The

9 Phone Directories Federal Court at [162]-[166].
10 Phone Directories Full Federal Court at [101], [102].
11 Phone Directories Full Federal Court at [7], [119].
12 Phone Directories Full Federal Court at [127].
13 *Fairfax v Reed* at [36].
14 *Fairfax v Reed* at [45].
15 *Larrikin Music Publishing v EMI Songs Australia* (2010) 263 ALR 155 (**Larrikin Federal Court**) at [82], [84].
16 Larrikin Federal Court at [80]-[81].

issue in relation to this contended work was whether authorship could be adequately established, and in particular whether joint authorship could be established. Fairfax argued that the article, headline and by-line were an individual work authored by the journalist responsible for writing the article and an unidentified sub-editor responsible for editing the article and creating the headline. Justice Bennett found that the evidence did not establish joint authorship of the article/headline combinations, as the writing of the articles and writing of headlines were distinct and separate tasks with different authors.[17]

## Substantial Part

### *Larrikin Music*

February 2010 was also the month the Federal Court handed down its judgment *in Larrikin Music Publishing v EMI Songs Australia* (2010) 263 ALR 155, a highly publicised case concerning two widely revered Australian songs 'Kookaburra Sits in the Old Gumtree' and Men At Work's 'Down Under'. This concerned a claim of copyright infringement, misleading and deceptive conduct and unjust enrichment by Larrikin Music Publishing against the composers of Down Under, and EMI Songs Australia and EMI Publishing (**EMI**) as the owner and licensee of copyright in the musical work.

At first instance, Jacobsen J found an objective similarity between the melodies of Kookaburra and Down Under, considering the works both aurally and visually.[18] In making this finding, the Federal Court applied the principle upheld in *IceTV* that substantiality focuses more on quality than quantity.[19] Larrikin Music failed on the claim of unjust enrichment[20] but succeeded on the claim of misleading and deceptive conduct under the Trade Practices Act, based on the finding that APRA AMCOS paid publisher and mechanical royalties to the Respondents as result of representations that they were wholly entitled to this income[21]. The fact that these representations to APRA AMCOS were continuing allowed Larrikin Music to circumvent the six-year statutory limit under the Act and claim loss and damage from May 2002 onwards.[22]

The Respondents appealed to the Full Federal Court of Australia on a number of grounds including that Jacobsen J had become a sensitized listener and that the Federal Court gave undue weight to the similarities between Kookaburra and Down Under and overlooked the differences. In April 2011, Emmett, Jagot and Nicholas JJ dismissed the appeal by the Respondents, upholding the finding the Down Under infringed the Larrikin's copyright in the musical work, Kookaburra.[23] Ultimately, the Full Federal Court found that the part reproduced was sufficiently significant to Kookaburra so as to constitute infringement and that "aural resemblance need not be resounding or obvious"[24] but would turn on the aural perception of the judge and the expert evidence.[25]

More broadly, this decision fanned the flames of those advocating for fair use exceptions (discussed below) or reducing the duration of the copyright, given the death of Kookaburra's composer Marion Sinclair 24 years earlier. As the Full Court remarked (per Jagot J):[26]

> *"One may wonder whether the framers of the Statute of Anne and its descendants would have regarded the taking of the melody of Kookaburra in the impugned recordings as infringement, rather than as a fair use that did not in any way detract from the benefit given to Ms Sinclair for her intellectual effort in producing Kookaburra."*

Special leave to the High Court was refused.[27]

## Authorisation

### *Roadshow v iiNet*

In *Roadshow v iiNet*, the bounds of the law of authorisation to sanction intermediaries were tested after first being applied to the internet environment in *Cooper* and *Kazaa* in the 2000s.

The film industry filed proceedings against an Australian ISP, iiNet, alleging it had authorised the infringements of its subscribers. At first instance, the Court found that the film industry had notified iiNet of instances where its subscribers (identified by IP address at certain times) were engaged in uploading or making available parts of films and television programs to other internet users via BitTorrent technology.

Justice Cowdroy found in favour of iiNet, introducing a concept new to the law of authorisation, namely "means of infringement".[28] He distinguished between the provision of access to the Internet (which his Honour regarded as the only relevant link between iiNet and the primary infringer, and therefore insufficiently proximate in nature) and the facilitation of the use of BitTorrent (which his Honour regarded as the true and proximate

17 Larrikin Federal Court at [101].
18 Larrikin Federal Court at [158]
19 Larrikin Federal Court at [42]
20 Larrikin Federal Court at [336]
21 Larrikin Federal Court at [284]
22 Larrikin Federal Court at [297]
23 *EMI Songs Australia Pty Limited v Larrikin Music Publishing Pty Limited* [2011] FCAFC 47 (**Larrikin Full Federal Court**).
24 Larrikin Full Federal Court at [86].
25 Larrikin Full Federal Court at [51].
26 Larrikin Full Federal Court at [101].
27 *EMI Songs Australia Pty Limited & Anor v Larrikin Music Publishing Pty Ltd* [2011] HCATrans 284.
28 *Roadshow Films v iiNet* (2010) 263 ALR 300 [400] (**iiNet Federal Court**).

means of infringement and not one that iiNet was relevantly responsible for). After reaching this conclusion, Justice Cowdroy also considered the factors under s 101(A) of the Act, finding that iiNet did not have the "relevant" power to prevent and that was not obtaining a financial benefit, and so did not have the necessary relationship with the primary infringer to be considered as 'authorising' the infringement.[29]

The film industry appealed to the Full Federal Court of Australia, with the matter heard by Emmett, Jagot and Nicholas JJ and judgment delivered on 24 February 2011. In a 2-1 split decision the Full Federal Court dismissed the appeal against the decision of the trial judge (Emmett and Nicholas JJ in the majority, Jagot J dissenting).[30] All three judges wrote separate judgments.

All three judges found that the trial judge had erred in his approach to both the legal test and the application of the law of authorisation.[31] They found that iiNet had the power to prevent the acts of infringement by sending warnings, suspending or terminating user accounts[32] and that such steps were reasonable.[33] The outcome of the appeal turned on how the majority approached a single issue, namely iiNet's knowledge of the infringements at the time of receipt of the notifications of infringement from the film industry. The majority of the Court (Emmett and Nicholas JJ) found that it was not unreasonable for iiNet not to act in response to the notices because the film industry had not provided "unequivocal and cogent" evidence of infringement and had not informed iiNet of the method of evidence collection prior to the filing of the proceeding[34] even though iiNet never intended to act on the notices.[35] Both judges ruled that the knowledge that iiNet acquired after the case was filed was irrelevant[36] overturning a contrary finding of the primary judge. This was despite criticisms of iiNet's approach to the allegations of infringement which "demonstrated a dismissive and, indeed, contumelious attitude".[37]

The decision also provided judicial support for a graduated response approach in Australia. Emmett J provided a 'roadmap' of steps that would oblige iiNet to act on infringements,[38] and the process that would be expected of iiNet in communicating with its customers. Some of this reasoning was picked up in later enquiries and industry negotiations, though it did not result in the introduction of an industry code setting out a graduated response scheme (see further below).

In dissent, Jagot J found that iiNet had the relevant knowledge because the notices from the film industry "provided credible evidence of widespread infringements of copyright" by iiNet users. iiNet's state of knowledge was "a product of iiNet's adopted position from the outset that it was not obliged to 'do squat'" in response to the notices "irrespective of the cogency of the information AFACT supplied".[39]

The film industry made a successful application for special leave to appeal to the High Court of Australia. The High Court's judgment was delivered on 20 April 2012.[40] In two judgments the High Court unanimously dismissed the appeal. In both judgments, the Court found that iiNet had not authorised the infringements of its users because it was reasonable for iiNet not to take steps to act in all of the circumstances (the judgments differed on the reasoning in relation to reasonableness, and reached the conclusions by reference to factors such as the nature of the internet and the BitTorrent system, the information that was provided to iiNet, its level of knowledge and the extent of its power to prevent). The majority judgment (French CJ, Crennan and Kiefel JJ) found that iiNet had only "indirect" power to prevent the infringements of its users, by terminating their contracts, and that the information in the notices from the film industry did not provide iiNet with a reasonable basis for sending warning notices to individual customers. The other judgment (Gummow and Hayne JJ) found that iiNet had limited control over the infringements and that the incomplete allegations notified to iiNet meant that it was not unreasonable for iiNet not to take action.[41]

The High Court identified the need for a legislative solution to the infringements, rather than by reliance on authorisation:[42]

> *This final conclusion shows that the concept and the principles of the statutory tort of authorisation of copyright infringement are not readily suited to enforcing the rights of copyright owners in respect of widespread infringements occasioned by peer-to-peer file sharing, as occurs with the*

29 iiNet Federal Court at [451].

30 *Roadshow Films Pty Limited v iiNet Limited* [2011] FCAFC 23 (**iiNet Full Federal Court**).

31 iiNet Full Federal Court, Emmett J [174]; Jagot J [401]; Nicholas J [694]-[700].

32 iiNet Full Federal Court, Emmett J [174]; Jagot J [426]; Nicholas J [720].

33 iiNet Full Federal Court, Emmett J [184]-[194]; Jagot J [408]-[415]; Nicholas J [748]-[749].

34 iiNet Full Federal Court , Emmett J [210]-[211].

35 iiNet Full Federal Court, Nicholas J [783]: "The fact that the respondent may not have acted on the AFACT notice even if they had contained additional information is besides the point".

36 iiNet Full Federal Court, Emmett J [210]-[211]; Nicholas [765].

37 iiNet Full Federal Court, Emmett J [210].

38 iiNet Full Federal Court, Emmett J [210].

39 iiNet Full Federal Court, Jagot J [405].

40 *Roadshow Films Pty Ltd v iiNet Limited* [2012] HCA 16 (**iiNet High Court**).

41 iiNet High Court at [146].

42 iiNet High Court at [79].

*BitTorrent system. The difficulties of enforcement which such infringements pose for copyright owners have been addressed elsewhere, in constitutional settings different from our own, by specially targeted legislative schemes, some of which incorporate co-operative industry protocols[84], some of which require judicial involvement in the termination of internet accounts, and some of which provide for the sharing of enforcement costs between ISPs and copyright owners.*

As will be seen below, despite numerous attempts, no such amendment to the law has been made in the 8 years since the High Court's decision in iiNet.

## The Communication Right

In the latter half of the decade, the Courts explored the scope of the communication right, and in particular the territorial nexus with Australia necessary in order to establish infringement of that right. In *Pokémon Company International, Inc. v Redbubble Ltd* [2017] FCA 1541 (**Pokemon v Redbubble**), Pokemon filed proceedings against Redbubble, an online marketplace that enables print on demand services with particular designs.

The proceedings concerned designs for clothing and other merchandise displaying the Pokemon characters (as well as associated images on the Redbubble website). The designs were uploaded to the Redbubble website and customers could visit the website and choose to have clothing and other merchandise made on demand displaying the Pokemon images.

A major issue in the case was whether there had been infringement of the communication right by Redbubble. Redbubble conceded that the relevant works had been communicated to the public, in the sense that that they were made available online and electronically transmitted, but argued that those acts were done by the artists who uploaded the works to Redbubble, rather than by Redbubble itself.[43]

Section 22(6) of the Act provides that a communication is taken to have been made "by the person responsible for determining the content of the communication" and the issue was previously considered in different factual scenarios by the Courts in *Cooper* (in relation to the operation of a website containing hyperlinks) and *iiNet* (where users were communicating cinematograph films via BitTorrent). In this case it was considered in the context of an online marketplace which relied on the provision of content by disparate artists.

The Federal Court found that while Redbubble did not provide the content of the works that were communicated to the public (as the artists did), Redbubble was responsible for determining that content through its "processes, protocols and arrangements with the artists".[44] However, Pokémon could not prove they should be entitled to damages for lost sales because the merchandise sold was a 'mashup'. Consequently, Pokemon was only awarded $1 nominal damages and no additional damages on the basis of policies in place that meant the infringement was not flagrant.

A similar case brought against Redbubble by the Hell's Angels Motorcycle Corporation (Australia) Pty Limited[45] failed because Hell's Angels could not establish copyright ownership.

## Preliminary Discovery

Against the backdrop of the *iiNet* decision, which meant intermediary ISPs were not likely to be liable for authorisation of copyright infringement, the attention of some rights holders turned to primary infringers. In 2014, the owners of the film "Dallas Buyers Club" commenced preliminary discovery proceedings against 6 Australian ISPs for the purpose of obtaining the details of customers associated with certain IP addresses that evidence established had been used to download and share copies of the film via BitTorrent. The application was strongly resisted by the ISPs.

The Federal Court held that Dallas Buyers had established the requisite elements to make out its application for preliminary discovery and ordered that the ISPs provide the details of the customers associated with the infringing IP addresses. The Court was satisfied that the evidence filed by Dallas Buyers established that there was a strong possibility that ISP customers were making available the film online via BitTorrent in infringement of the communication right.[46] However, Justice Perram placed a significant and unusual limitation on his orders in this regard. To prevent what was termed "speculative invoicing", Dallas Buyers was required to clear with the Federal Court any correspondence it proposed to send to the identified customers.[47]

The Court's assessment of the proposed letters was particularly involved. Justice Perram concluded that certain types of demand were acceptable, but ruled out any licence fee damages and additional damages. The Court also required a written undertaking that Dallas Buyers would restrict its demands to those the Court had ruled as acceptable (limited to compensation for the price of the film and costs for the legal proceedings).[48] In addition, as Dallas Buyers was not an Australian company, the Court required that the undertaking be secured by the lodging of a $600,000 bond.[49]

This level of judicial oversight of what a successful preliminary

43 Pokemon v Redbubble at [46].
44 Pokemon v Redbubble at [48].
45 *Hells Angels Motorcycle Corporation (Australia) Pty Limited v Redbubble Limited* [2019] FCA 355.
46 *Dallas Buyers Club LLC and another v iiNet Ltd and others* (2015) 327 ALR 670 at 689
47 *Dallas Buyers Club LLC and another v iiNet Ltd and others* (2015) 327 ALR 670 at 689
48 *Dallas Buyers Club LLC and another v iiNet Ltd and others* (No 4) (2015) 327 ALR 702 at [34]
49 *Dallas Buyers Club LLC and another v iiNet Ltd and others* (No 4) (2015) 327 ALR 702 at [35]

discovery applicant may do with information it obtains was unprecedented. Justice Perram also stated that his reasons should apply in all future applications where a rights holder seeks access to user details from an ISP via a preliminary discovery application and that applicants would need to put on evidence regarding the nature of the demands they propose to make to the infringing ISP customers.[50]

Ultimately, the Dallas Buyers litigation was an attempt by a rights holder to seek access to documents to identify the individuals involved in copyright infringement, but that attempt was fundamentally frustrated when the Court pre-set limits on the damages that could be recovered (without proceedings even being issued against those individuals or any evidence of the scale of actions by the individual infringers) and imposed an unprecedented requirement that the copyright owner pay an extremely significant bond into Court.

## Legislative Amendments and Review

### Section 115A

While rights holders failed to hold intermediaries liable for authorisation of infringement by users (*iiNet*) and struggled to obtain preliminary discovery orders identifying infringers without costs prohibitive investment (*Dallas Buyers*), they and other stake holders continued to pursue a site blocking regime in Australia.

*The Copyright Amendment (Online Infringement) Act 2015* (Cth) commenced as law on 27 June 2015 after being passed by Parliament with bipartisan support. It amended the Act by incorporating a new s 115A which empowered rights holders to seek injunctive relief to require a carriage service provider (**CSP**) to take reasonable steps to disable access to certain online locations. The site blocking provision followed the introduction of similar provisions in the UK and Singapore.

In order to obtain an injunction under section 115A, a content owner must satisfy the Court that:

- a carriage service provider provides access to an online location outside Australia;
- the online location infringes, or facilitates an infringement of, the copyright; and
- the primary purpose or primary effect of the online location is to infringe, or to facilitate the infringement of, copyright (whether or not in Australia).

Further, the Court must also consider the list of matters in s115A(5) when determining whether to order an injunction. The list includes the flagrancy of the infringement, whether access to the online location has been blocked in other jurisdictions and whether disabling access is a proportionate response and in the public interest.

Since the introduction of s 115A a number of applications by rights holders have been successfully made requiring ISPs to block access to certain online locations.[51]

The introduction of the site blocking regime was a solution which sidestepped the issue of liability of intermediaries and even infringers, to create a no-fault regime designed to prevent and inhibit infringement online.

Short comment about extension to search engines?

### Legislative Review

Over the past decade there have been multiple legislative reviews into various areas of copyright law. They include:

- Australian Law Reform Commission, *Copyright and the Digital Economy* (Report No. 122 November 2013);
- Australian Government (Cth), *Online Copyright Infringement Discussion Paper* (July 2014), which contributed to the introduction of section 115A and the attempted Industry Code Negotiations (facilitated by Communications Alliance);
- Senate Legal and Constitutional Affairs Legislation Committee, *Copyright Amendment (Online Infringement) Bill 2015* (11 June 2015);
- Productivity Commission, *Inquiry Report into Intellectual Property Arrangements* (Report No. 78, December 2016);
- Department of Communications and the Arts, *Review of Copyright Regulations 1969 and the Copyright Tribunal (Procedure) Regulations 1969* (September 2017);
- Department of Communication and the Arts, *Review of Copyright Online Infringement Amendment* (February 2018);
- Department of Communication and Arts, *Consultation on draft Copyright Amendment (Service Providers) Regulations 2018 to implement Safe Harbour Reforms* (June 2018);
- Bureau of Communications and Arts Research, *Review into the Code of Conduct for Copyright Collecting Societies* (Report, April 2019)'
- Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (July 2019); and
- Department of Infrastructure, Transport, Regional Development and Communications, *Copyright Modernisation Review* (ongoing).

50 *Dallas Buyers Club LLC and another v iiNet Ltd and others* (No 4) (2015) 327 ALR 702 at [36]

51 *Roadshow Films Pty Ltd v Telstra Corp Ltd* (2016) 122 IPR 81 (Solarmovie websites, The Pirate Bay websites, Torrentz websites, TorrentHound); *Universal Music Australia Pty Ltd v TPG Internet Pty Ltd* (2017) 126 IPR 219 (Kickass Torrents); *Australasian Performing Right Association Ltd v Telstra Corp Ltd* (2019) 369 ALR 529 (injunctions granted in relation to websites which allowed users to rip streamed content from YouTube); *Foxtel Management Pty Ltd v TPG Internet Pty Ltd* (2019) 148 IPR 432 (ShareMovies, SeriesOnline8, Movie4U, SeeHD, StreamDreams, MoviesOnline, WatchSoMuch, TorrentKen, SkyTorrents, Unblocked.lol, Unblocked.win, Unblockall, Unblocker and Myunblock).

Arising from these reviews and enquiries have been many recommendations about amendments to copyright law in Australia. Those include the introduction of a fair use exception (ALRC's Copyright and the Digital Economy, Productivity Commission's Inquiry into Intellectual Property Arrangements and being considered in the Copyright Modernisation Review), the introduction of an industry code to govern the steps ISPs should take in relation to infringement by users (Online Copyright Infringement Discussion Paper), the introduction of a site blocking regime (Online Copyright Infringement Discussion Paper) and the implementation of a mandatory takedown scheme (ACCC Digital Platform Inquiry). Of the many recommendations made the only significant legislative change to copyright law in the last decade has been the introduction of the site blocking regime described above. The remainder of the recommendations have either been taken on notice (such as fair use), stymied by lack of agreement by stakeholders (the industry code) or rejected by government (the takedown scheme).

## The 2020s

### Love is in the Air

The first significant copyright judgment of this new decade is likely to be the Federal Court's decision in the Love is in the Air case, which commenced in 2019.

This case was brought by the copyright owner of the iconic Australian disco song *Love is in the Air* Boomerang Investments Pty Ltd, written by Harry Vanda and the late George Young in 1977 (**LIITA**). Vanda & Young (by his personal representative) were co-applicants in the proceedings and APRA AMCOS were joined shortly before the hearing commenced as the Fourth and Fifth Applicants.

The First and Second Respondents are John Padgett and Lori Monahan, an electro pop duo known as Glass Candy. Between 2005-2011, John Padgett composed the music and Lori Monahan wrote the lyrics for the song *Warm in the Winter* (**WITW**). The song is 6'45" long and the words "love/s in the air" feature in its lyrical content.

The Applicants alleged that WITW contains a reproduction of a substantial part of the literary and musical works that comprise LIITA and that Glass Candy streamed (communicated) and authorised the download (reproduction) of WITW by internet users in Australia.

The musical work allegation was that the music accompanying the words "love is in the air" had been copied (the hook). At the trial, the Applicants also alleged that WITW copied the entirety of the music corresponding to the words "love is in the air, everywhere I look around/ love is in the air, every sight and every sound" (the head). It was submitted that that hook and the head reproduced a substantial part of LIITA's musical work. Glass Candy's sub-publisher in Australia (Kobalt) was joined as the Third Respondent. The Applicants further alleged that a version of WITW titled *France is in the air* (**FIITA**) that was licensed to the fourth respondent, Air France for use in an international advertising campaign infringed LIITA for the same reasons and was streamed and played as music on hold in Australia.

The Court heard from two musicologists in the expert conclave which centred around the analysis of the hook and the head, and competing views about the originality of musical concepts found in both songs such as intervals, chord progressions, rhythmic definitions, tempo, metre and key.

Key issues the Court will determine include:

- if the evidence of independent creation of WITW is accepted;
- whether the hook and the head are original and whether they reproduce a substantial part of LIITA's musical work (on their own and as repeated and varied throughout the song);
- whether the literary work comprising the lyrics 'love is in the air' was infringed in WITW in circumstances where evidence of the ubiquity of the phrase, both pre- and post-LIITA, was led by the Respondents;
- whether Air France's evidence of independent creation of the phrase "France is in the air" and development of FIITA is accepted;
- having regard to the various arrangements between composers, copyright owners and APRA AMCOS, who owns the relevant parts of the copyright in musical and literary works and who has standing to sue in music copyright cases; and
- the scope of the communication right (ie who is determining the content of the communication per s 22(6)) and its territorial connexion to Australia).

A point of discussion at the hearing that may feature in the judgment is whether lyrics and music can be considered together for the purposes of assessing infringement of musical works, akin to the position in US where the definition of "musical work" explicitly includes "accompanying words":

The hearing concluded in June 2019 and judgment is pending.

### Where to from here

The last decade explored the scope and limits of copyright on the internet, setting limits on the liability of intermediaries while confining what material can be protected by copyright, including confirming that human authorship is required for subsistence. In the next decade, as we see further development of works involving computer generated elements and the use of artificial intelligence, we can expect to see cases exploring the complexities of identifying that human element, and increased pressure in relation to the need to protect valuable works in this category, including potentially by way of a database right.

# National Security and Tech: The New Decade

**Patrick Fair,** principal at Patrick Fair Associates, comments on the developments at the intersection of national security and tech between 2010-2019, and on what's on the agenda in this space for the next decade.

## 1. Introduction

Australia's national security regime has developed significantly over the last decade. The government introduced significant new powers to fight terrorism and a range of measures focused on identifying and protecting Australia from foreign interference. Some significant changes were made to respond to technological change while others aimed at making national security agencies and law enforcement more efficient and effective.

This short article provides an overview of the key national security changes introduced over the last decade and of the changes that are in the pipeline. In the conclusion, there is an outline of some of the issues that might drive further change.

## 2. The Decade Past: laws to fight terrorism

During the early part of the decade developments in Syria and Iraq and news that some Australians had travelled to fight with Da'esh resulted in the introduction of the new penalties and expanded powers to address terrorism.

In 2010 the *National Security Legislation Amendment Act 2010* amended a number of Acts to adjust treason and sedition offences, to clarify when an organisation advocates the doing of a terrorist act, to add powers to search premises in relation to terrorism offences, re-entry of premises in emergency situations, bail for terrorism and national security offences and more.

The *Counter-Terrorism Legislation Amendment (Foreign) Fighters Act 2014* amended the meaning of 'terrorism offence' in the *Crimes Act 1914*, extended the power to arrest without a warrant and introduced the delayed notification search warrants, made a new offence of advocating terrorism, changed and extended the control order and preventative detention order regimes, and introduced stop, search and seizure powers relating to terrorism offences. The Act also introduced a new offence of 'publicly advocating genocide' to people inside or outside Australia, carrying a maximum sentence of seven years' imprisonment. ASIO was given a new questioning and detention warrants regime and changes were made to the *Foreign Evidence Act 1994* to provide greater discretion in admission of foreign material in terrorism-related proceedings. You might recall the public controversy over the new offence of disclosing information relating to warrants or execution of a warrant introduced to the *Criminal Code* as 3ZZHA due to concern regarding the impact on reporting of news.

On 11 December 2015 assent was given to the *Australian Citizenship Amendment (Allegiance to Australia) Act 2015* which describes certain terrorist related activity by a dual citizen as constituting a renunciation of Australian citizenship and/or giving rise to a ministerial power to cancel Australian citizenship.

On 29 November 2016 the *Counter-Terrorism Legislation Amendment Bill (No.1) 2016* received assent introducing further extensive changes to the *Criminal Code* control order provisions including adding provisions to effectuate the use of tracking devices on persons the subject of control orders and expanding powers to monitor compliance.

On 7 December 2016 the *Criminal Code Amendment (War Crimes) Act 2016* received assent. This Act amends Division 268 of the *Criminal Code* to align Australian domestic law with international law in relation to the treatment of members of organised armed groups in non-international armed conflict. The Act amends Division 268 of the *Criminal Code* to give effect to Australia's obligations as a party to the *Rome Statute of the International Criminal Court.*

Also on 7 December 2016 assent was given to the *Criminal Code Amendment (High Risk Terrorist Offenders) Act 2016* which introduced *a* framework into Part 5.3 of the *Criminal Code* for the continued detention of high risk terrorist offenders serving custodial sentences who are considered by a court to present an unacceptable risk to the community.

Towards the end of the decade the operation of anti-terrorism laws with sunset dates was extended by three years to 7 September 2021 by the *Counter-Terrorism Legislation Amendment Bill (No. 1) 2018*. This Act extended the operation of control order regime in Division 104 of the *Criminal Code*, the preventative detention order regime in Division 105 of the *Criminal Code*, the declared area provisions in sections 119.2 and 119.3 of the *Criminal Code*, and the stop, search and seizure powers in Division 3A of Part IAA of the *Crimes Act 1914*. In addition, new laws intended to combat terrorism focused on the perceived risk posed by radicalised Australians returning home.

The *Crimes Legislation Amendment (Police Powers at Airports) Act 2019* received assent on 28 October 2019. This Act enables police to direct the presentation of evidence of identity by persons at major airports. The

police are also given power to issue move-on and stop directions.

Two other terrorism related bills were prepared and introduced before the May 2019 election but have not been reintroduced at the time of writing. The *Counter-Terrorism (Temporary Exclusion Orders) Bill 2019*. The simplified outline describes the purpose of the bill as "The Minister may make an order (called a temporary exclusion order) that prevents a person from entering Australia for a specified period, which may be up to 2 years. An order cannot be made unless certain conditions are met, and it can be revoked."

## 3. The Decade Past: laws for surveillance, evidence gathering and agency powers

In May 2012 the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) was requested to conduct an inquiry into the reforms of Australian's National Security legislation. The PJCIS report was published on 24 June 2013 and the government responded on 1 July 2015. Many of the major changes to surveillance, evidence gathering and agency powers that took place in the remainder of decade came from or were related to recommendations by PJCIS in its report.

The *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* received assent on 13 April 2015 introducing a 2 year mandatory data a retention obligation for services "carrying communications, or enabling them to be carried" provided by carriers and carriage service providers. The data that must be retained includes user details, destination, date and time, and the type of service used. Being data rather than "content" this information is accessible to listed enforcement agencies and some state authorities with independent powers of access by issuing an authorisation. A warrant is not required. Importantly, an enforcement agency cannot issue an authorisation for access to metadata if the issuing party knows or reasonably believes the person to be working in the capacity of a journalist or is the employer of such a person and the purpose of the authorisation is to identify a source unless a journalist information warrant has been issued according to certain public interest criteria. According to the relevant *Telecommunications (Interception and Access) Act 1979* (**TIA Act**) Annual Reports, 2 Journalist Information Warrants allowed 58 authorisations in 2017/18 and 6 allowed 20 authorisations in 2018/19. The data retention laws are subject to automatic review by the PJCIS. A review is currently underway and due to report 30 June 2020.

The *Telecommunications and Other Legislation Amendment Act 2016* report 2017 received Assent on 18 September 2017 introducing national security related amendments to the *Telecommunications Act 1997* (**Telecoms Act**). These amendments are known as the telecommunication security sector reforms or TSSR. The TSSR create an obligation on carriers and carriage service providers to "do their best" to:

> "…protect telecommunications networks and facilities owned, operated or used by the carrier or provider from or unauthorised interference or unauthorised access to ensure the:
>
> (c) confidentiality of communications carried on and of information contained on, communications networks or facilities; and
>
> (d) availability and integrity of communications networks and facilities."

The obligation extends to requiring a carrier or carriage service provider to notify the Department of Home Affairs if it proposes to make any change to its networks or facilities which may be adverse to security. Carriers and nominated carriage service providers can notify Home Affairs and receive an indication of whether or not Home Affairs has any concern. If there is an indication of concern and the carrier does not remediate as recommended by the department, the Minister has a broad power to negotiate or seek a security assessment from ASIO, which if adverse, allows the Minister to direct the regulated entity to comply (or take any other steps).

On 23 August 2018 the Minister issued "5G Security Guidance" to Australian carriers referencing the TSSR which included the statement "The Government considers that the involvement of vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law, may risk failure by the carrier to adequately protect a 5G network from unauthorised access or interference." With reference to this statement but, apparently without any other formal action by the government, TPG announced it would not use Huawei or ZTE equipment in its network.

The *Security of Critical Infrastructure Act 2018* received assent on 11 April 2018. This Act introduced a scheme to improve the national security posture of specified ports, qualifying power generation gas supply and water facilities. The Minister has power to declare other infrastructure subject to the regime. The owners and operators are required to prepare and file with Home Affairs information regarding their identity (including their nationality) and the same information in relation to shareholders with a specified holding and all controlling entities. The information must be updated within 30 days of any substantive change. The Minister has the power to make directions regarding ownership or operation of the asset should the Minister obtain an adverse determination by ASIO that a matter notified is adverse to national security. This power could

be used to direct asset owners or operators to transfer their interest or to bring onshore or implement replacement technical solutions.

The *Foreign Influence Transparency Scheme Act 2018* received assent on 29 June 2018. This regime requires a person acting on behalf of foreign government or political organisation to register with the Commonwealth. The Act does not require foreign entities who happen to be foreign owned or controlled to register and does not require registration by business contractors not engaged in communications, advocacy or lobbying. After the introduction of this scheme lobbyists, advocates and lawyers engaging in policy work must take care to establish the ownership and control of their clients.

*National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* received assent on 30 June 2018. This Act amended the *Criminal Code* to add new offences related to treason and espionage. The Act introduced offences for public servants acting against the Australian national interest and generally applicable offences of being reckless regarding Australian national security when dealing with certain information and certain foreigners. Responding to the potential impact of the new offences, a multinational university research project was formed and, in November 2019, *Guidelines to Counter Foreign Interference in the Australian University Sector* were published.

The *Telecommunications and Other Legislation Amendment (Assistance and Access Act 2018* received assent on 8 December 2018. Also known as the "Encryption Act" this Act introduced a new Part 15 to the Telecoms Act and made significant amendments to the *Surveillance Devices Act 2004* and the *Australian Security Intelligence Organisation Act 1979* (amongst many others) directed at improving the effectiveness and agility of national security and law enforcement agencies. The new Part 15 introduces a new wide class of regulated entities called "designated communications providers" (DSPs). DSPs include carriers, carriage service provides and a wide range of electronic services, software, equipment and facilities providers involved with systems that carry communications. Listed agencies called "interception agencies" can request or require assistance from DSPs including removing one or more forms of electronic protection, providing technical information, installing, maintaining or testing the using of software and equipment as well as facilitating objectives of the relevant agency. This Act passed on the last day of Parliament in 2018 subject to an informal agreement between the government and the Labor Party that certain matters would be addressed. There is currently a Bill before parliament proposing a series of amendments and a government initiated a review conducted by the PJCIS which has been referred to the Independent Security Legislation Monitor (**ISLM**). The ISLM has been taking submissions and has indicated an intention to report by 30 June 2020.

Towards the end of the decade the government established the Home Affairs portfolio and increased the power of national security agencies including by passing the *Home Affairs and Integrity Agencies Legislation Amendment Act 2018*. Home Affairs is responsible for immigration, border protection, domestic security and law enforcement agencies. The Act also reformed the Attorney-General's oversight of Australia's intelligence community and agencies in the Home Affairs portfolio. There was also *Intelligence Services Amendment Act 2018* which enables the Minister to protect persons outside Australia with an Australian Secret Intelligence Service (**ASIS**) member or agent and authorise the ASIS staff member to use "reasonable and necessary force" in the performance of his or her functions.

## 4. Changes on the Horizon

Use of facial recognition technology by government services is on the way. In October of 2019 the PJCIS issued an advisory report on the *Identity-matching Services Bill 2019* (**IMS**) and the *Australian Passports Amendment (Identity-matching Services) Bill 2019 (***Passports Bill***)*. The IMS seeks to establish services to identify, recognise or verify facial images and systems for collection, access, use, sharing and disclosure related data. The Department of Home Affairs would create and maintain facilities for the sharing of facial images and other identity information between government agencies, and in some cases, non-government entities. It will support a federated database of information contained in government identity documents such as driver licences.

Although expressing support for the rationale behind each bill, the PJCIS recommended that the IMS be redrafted to create a regime built "around privacy, transparency and subject to robust safeguards", to improve transparency, reporting and to clearly state the obligations of participating parties. The PJCIS also recommended that the *Passports Bill* be amended to ensure that automated decision making could only be used for decisions that produce favourable or neutral outcomes for the subject, and that such decisions would not negatively affect a person's legal rights or obligations, and would not generate a reason to seek review.

In a recent hearing on the Encryption Act, the ISLM gave an opening statement that indicated some thinking on changes to the Act. In particular, he appears in favour of some form of judicial supervision of requests and notices issued under Part 15 of the Telecoms Act including a review process that might publish reasons for decisions made in order to provide public guidance improved clarity of the limiting terms "systemic weakness" and "systemic vulnerability" by inclusion of statutory examples in the law. The views of the ISLM

suggest that some of the sought after improvements of the Encryption Act may eventuate.

On 7 October 2019, there was a joint statement issued by US Attorney General William Barr and the Minister for Home Affairs, Peter Dutton on the US Cloud Act. On 5 March 2020 the federal government introduced the *Telecommunications Legislation Amendment (International Production Orders) Bill 2020* in the House of Representatives. The proposed new law will allow Australian law enforcement and national security agencies to issue international production orders (**IPOs**) to communications service providers outside Australia in certain circumstances and facilitates compliance with IPOs from offshore by telecommunications providers in Australia.

## 5. Issues for the future

Without a crystal ball and not being a member of our national security apparatus the writer is not in a good position to predict what further controls and powers the Minister and our agencies might wish to legislate. I can however comment on some areas that clearly require careful attention:

- **The distinction between metadata and content.** The Attorney General responsible for introducing the mandatory data retention regime famously underplayed the power of metadata by comparing it to the information on the outside of an envelope. Under the existing regime national security and law enforcement bodies access up to 2 years of historical metadata and identify future metadata in real time without a warrant. It might be argued that some information about an electronic device is less privacy intrusive than some things a person might say while using the device. However, a real time feed of metadata from a person's device and/or 2 years of data indicating where they have been, who they called and how long they spoke to them, is not less privacy inclusive. It currently requires a warrant to place a tracking device on an individual's person or property but two years of metadata can be obtained on written request. The information content of metadata was highlighted in a recent answer by the Commonwealth Ombudsman, Michael Manthorpe, to a question raised in the PJCIS review of the mandatory data retention regime. Mr Manthorpe reported that metadata being supplied to agencies included the full URL being visited and therefore indicated content being viewed by the subject individual.
- **The meaning of "communication"**. The Telecoms act defines the word "communication" inclusively to cover a conversation and a message whether in the form of sounds, data, text, visual images or signals. This definition does not sit well with the mandatory data retention regime or the TIA Act because it captures data and machine messages that should not be subject to regulation or storage and, in particular, may create unreasonable regulatory obligations for IoT networks
- **Regulation of direct access to information systems.** Our legislation presumes that agencies cannot obtain third party information except by request or compulsory acquisition. However, the Encryption Act now gives interception agencies the power to install or have built their own direct access to third party information. If such a point of access was constructed, the agency would not have to require data by warrant or authorisation, it could be collected or delivered by the technology of the agency. s317ZH (1) to the Telecoms Act attempts to address this issue by expressly maintaining existing requirements to use a warrant or authorisation to obtain data but considering the step change in agency power introduced by the Encryption Act (i.e. the ability to install software or equipment on a third party system without a warrant) it may be unnecessary to request data from a designated communication provider at all. The Encryption Act appears to open a major gap in the information security framework.
- **The role and regulation of surveillance**. The TIA Act authorises the disclosure of prospective telecommunication data. According to the latest report on the TIA Act for 2018/2019, 27,824 authorisations for prospective data were issued during the period of the report. The writer understands that when prospective data is requested, it may be provided in real time. If the data provided includes information in the mandatory data retention data set (which would seem likely) the provision of prospective information clearly amounts to real-time surveillance of the location and calling activity the subject of the authorisation. The powers in the Encryption Act could be used to obtain a similar feed of real time information from over-the-top service providers. Considering that the Australian Securities and Investment Commission currently monitors the trading on the Australian Stock Exchange in real time for insider trading using a data analytics engine, we might reasonably expect our national security and law enforcement agencies to seek to review "prospective data" in bulk to look for patterns and behaviours that indicates unlawful activity. Considering such data could be obtained with a single prospective authorisation issued on the agency's own initiative, this may be happening already.

- **Protection of a free press.** The journalist information warrant regime in the TIA Act does not prevent the use of metadata to identify a journalist's source unless the authorisation pertains to the data of a journalist or his or her employer. In addition, the journalist warrant regime does not moderate the other various criminal offences that prevent publication of information about national security activities and operations even when to do so would be in the public interest. A discussion paper by The Alliance for Journalists' Freedom advocates a Media Freedom Act aimed at "striking the right balance in National Security Legislation". Calls for moderation of national security laws to protect journalists and a free press are likely to persist.
- **Adverse impacts on industry.** Two examples:
    - Encryption and security tool developers in Australia expressed alarm regarding the Encryption Act because the law gives interception agencies the ability to access, copy and amend the source code of their products making them potentially undesirable. At one industry forum, the CEO of a leading software company said that he was being forced to move all development offshore.
    - The mandatory data retention regime imposes an onerous retention obligation on any communication service provider that happens to resell carriage. This creates a strong incentive for system integrators and data centre providers to avoid selling carriage to their customers even when it would be profitable to do so. The adverse impact of the existing regimes on Australian industry is likely to remain a basis for reform of these regimes in the coming decade.

More broadly, during consultations on Australia's 2020 Cyber Security Strategy it has been suggested that key strategic information systems should be hardened by a new TSSR type system protection obligations or the imposition of standards or a code.

## 6. Conclusion

Our national security laws have been changing rapidly in a rapidly changing environment. With this in mind, it is neither surprising that many aspects of the regime have raised serious issues nor that many aspects are subject to ongoing review and have further significant changes on the horizon.

**Patrick Fair** is the principal of Patrick Fair Associates, an Adjunct Professor at the School of Information Technology, Faculty of Science, Engineering and Built Environment at Deakin University, the Chairman of the Communications Security Reference Panel at the Communications Alliance, and General Advisor for LexisNexis Practical Guidance Cybersecurity, Data Protection and Privacy.

# 2020 CAMLA Young Lawyers Networking Event

By CAMLA Young Lawyer Committee representative **Amy Campbell** (Senior Associate, HWL Ebsworth)

From a time when groups of more than 2 people could meet publically, on the evening of 24 February 2020, Clayton Utz generously hosted the 2020 CAMLA Young Lawyers Networking event.

From what is now an unfathomably large number of people gathered in one (albeit large) room, more than 100 young lawyers and law students attended to hear from the panel of leading lawyers within the media and communications industry, to develop existing relationships and expand their networks for relationships for the future.

The esteemed panellists - Claudia Wallman (Senior Legal Counsel, Spotify), Monique Hennessy (Legal Counsel, NRL), Neil Murray SC (Tenth Floor Chambers) and Robyn Ayres (CEO, Arts Law Centre of Australia) - emphasized the values of the authenticity, sincere relationships and keeping an open mind at each stage of their careers.

The audience heard the leading panellists recount important steps taken in their careers, offer insights and tips on networking and nurturing professional relationships, and reflect on critical guidance they have received from mentors and key contacts during their careers.

Some key insights include:

- Networks are about using resources available to you to solve problems.
- Networks aren't just about you - how can you help and connect others?
- Keep an open mind about what you can learn at any point in your career and by completing any task - even doing due diligence, you can learn so much about a company.

The Young Lawyers Committee again expresses our gratitude to the excellent panellists for sharing their time and insight, to the engaging moderators - our very own Isabella Street (Sony Music) and Patrick Tyson (ABC) who organised the event with Calli Tsipidis (Legal Counsel, FOX Sports) and Katherine Sessions (Senior Legal & Policy Advisor, e-Safety Commissioner), and to Tim Webb (Partner, Clayton Utz and CAMLA Board member) and Clayton Utz for their hospitality and generosity in hosting.



# A New Decade of Data Privacy

**Eli Fisher,** Senior Associate at Baker McKenzie, discusses the main developments in data privacy law in the 2010s and comments on what lies ahead in the 2020s.

## Introduction

Data privacy sits today atop the regulatory agenda of many countries around the world. But it wasn't always this way. In fact, it is hard to think of an area of law that has leapt so decisively as did privacy law from peripheral to central in the concerns of regulators, businesses and individuals in the previous decade.

It's an interesting exercise to break things up by decades, as Sam Seaborn once did when advising on the nomination of a Supreme Court justice at the turn of the millennium:

> *It's not just about abortion, it's about the next 20 years. In the '20s and '30s it was the role of government. '50s and '60s it was civil rights. The next two decades are going to be privacy. I'm talking about the Internet. I'm talking about cell phones. I'm talking about health records and who's gay and who's not. And moreover, in a country born on the will to be free, what could be more fundamental than this?*

Two decades ago, in the year 2000, the Office of the Privacy Commissioner was established, and the *Privacy Amendment (Private Sector) Act 2000* extended coverage of the Privacy Act to some private sector organisations and introduced 10 National Privacy Principles. (I know. It doesn't have the same soaring Sorkinesque cadence as the way Sam put it.)

A decade later, the ALRC's *For Your Information* report was continuing to shape privacy policy, as it had been since August 2008 when it was first released to the public. That report with its 295 recommendations set in motion the reforms to the law that we have today.

## APPs

In 2012, Attorney-General Nicola Roxon circulated the explanatory memorandum to the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth), which would explain the greatest changes to Australian privacy law to date. In response to the ALRC's report, the Bill would eventually amend the Privacy Act to create the APPs, a single set of privacy principles applying to both federal government agencies and private sector entities. The APPs replaced the federal public sector's IPPs and the private sector's NPPs that had previously governed the handling of personal information. The Bill also introduced more comprehensive credit reporting with improved privacy protections, introduced new provisions on privacy codes and clarified the functions and powers of the Privacy Commissioner.

These amendments took effect on 12 March 2014. Some of the most noteworthy changes were the introductions of APP 1 and APP 5, which forced APP entities to be more transparent about their handling of personal information, through privacy policies and collection notices. We were also introduced to the requirement under APP 2 to permit pseudonymity and anonymity where practicable. APP 7 enhanced the requirements for informed user consent in relation to direct marketing. And APP 8 proposed to hold the APP entity that transfers personal information overseas accountable for the conduct of the overseas recipient. The Privacy Commissioner was buttressed by new powers, including the ability to obtain enforceable undertakings, to seek civil penalty orders and to obtain injunctive relief.

These reforms were game-changing. But they left certain issues unresolved. When is information about a person as opposed to a device or a network? Is a voluntary data breach notification scheme sufficient? Do the penalties and enforcement powers of the Privacy Commissioner give privacy law enough teeth to warrant serious corporate attention? Can privacy really be protected by territorial laws, or is it necessary to take an international or extraterritorial approach to regulating data processing? Can consent really be the silver bullet for data handling in this day and age? Do individuals need the ability to protect their privacy directly, or can reliance be placed on a Data Protection Agency, such as the Privacy Commissioner? These questions would continue to arise throughout the decade.

## Grubb

In 2013, still under the previous NPP framework, Ben Grubb a Fairfax tech journalist made a request for the metadata that Telstra, his mobile phone provider, held about him. This was back in the day when the Government was working on the introduction of the mandatory data retention laws requiring telcos to retain metadata on their customers for two years. Grubb was curious as to what metadata was being collected. Telstra provided some information, but refused to provide its mobile network data, which included metadata such as IP addresses and, most crucially, geolocation data.

Grubb responded by lodging a complaint with the Privacy Commissioner. Telstra maintained that the geolocation data it had for Grubb - the longitude and latitude of mobile phone towers connected to the phone at any point in time - were not personal information about a customer. Telstra's argument was that the data were

about the device, not about Grubb. The Privacy Commissioner found against Telstra in May 2015 on the basis that Telstra could cross-match different datasets allowing Grubb to be linked back to the geolocation data of his phone.

Telstra appealed the Privacy Commissioner's decision to the AAT, and was successful. Basically the arguments here dealt with whether the information Grubb was seeking, and Telstra was withholding, was 'personal information' as defined by the Privacy Act. The definition of personal information (which has since changed) relevantly referred to information about an individual whose identity is apparent, or can reasonably be ascertained from the information. The parties had argued about whether Grubb's identity could reasonably be ascertained from the network data, which depended on the cross-matching efforts Telstra would need to go to, to ascertain Grubb's identity. The AAT held that the network data that Grubb was seeking was not information about Grubb, but information about the service Telstra was providing to Mr Grubb.

The Privacy Commissioner appealed the AAT's decision to the Full Court and lost (as, incidentally did everyone who wanted clarity on these important questions). The Full Court could only answer questions of law, and did not accept the Privacy Commissioner's interpretation of the definition of 'personal information'. But it did not determine whether the information in question was 'about' Grubb, or whether Grubb's identity could reasonably be ascertained from the metadata. And thus, the most authoritative review of the centrepiece of privacy law - 'personal information' - ended with no great clarity. The Privacy Commissioner released a public statement welcoming the decision as it provides important guidance as to what is 'personal information': "In particular, the Court has confirmed that assessing what is 'personal information' requires an 'evaluative conclusion, depending on the facts of any individual case' and that 'even if a single piece of information is not 'about the individual' it may be about the individual when combined with other information'."

## GDPR

The General Data Protection Regulation (**GDPR**) came into force on 25 May 2018 in all member states of the European Union, and brought along a new regime of data protection laws - and large penalties - that replaced all existing privacy law in the European Union. It was approved and adopted on 14 April 2016 by the European Parliament, giving businesses over two years to prepare for significant changes.

The GDPR is an ambitious regime which aims to harmonise data protection laws across the EU, while enhancing the protections afforded to the privacy of people in the EU. The regime was described as the most important change in data privacy regulation in 20 years.

Much can and should be said about this significant development, including in relation to the mandatory data breaches scheme, the lawful bases for processing under Article 6, which require any processing of personal information to be justified by one of the listed lawful bases and expressly so, and the individual rights which captured much of the media attention surrounding the GDPR. The GDPR provided to individuals the right to be informed about the personal data an organisation holds about them; to access the personal data; to rectify the data; to have the data erased (otherwise known as the right to be forgotten); to restrict processing of personal data; to data portability; to object to the processing of personal data; and rights in respect of protection from automated decision making, including profiling.

The GDPR also changed the privacy game by providing for penalties that are starkly unfamiliar to Australian privacy practitioners. Under the GDPR, there are increased administrative fines for non-compliance: serious contraventions can result in penalties of up to €20 million or 4% of annual worldwide turnover (whichever is higher), and less serious contraventions can result in penalties of up to €10 million or 2% of annual worldwide turnover (whichever is higher). Penalties under the GDPR are in sharp contrast to those available under the Privacy Act, which (at least currently) gives the Privacy Commissioner enforcement powers including maximum civil penalties of up to $2.1 million. Ordinarily, privacy complaints in Australia are resolved with limited financial cost to the infringer, by way of penalty or compensation.

But perhaps the most interesting aspect of the GDPR both generally and for practitioners here in Australia is its purported extraterritorial reach. An Australian business needs to comply with the GDPR if it: (a) has an establishment in the EU; or (b) targets people in the EU, either in relation to the offer of goods or services to them or in relation to monitoring their behaviour. Thus, it is necessary for businesses in Australia to apply not just the standards of the Australian privacy law to their data processing, but also in certain circumstances the stricter foreign standards of the EU.

As with the former Data Protection Directive, the GDPR imposes restrictions on the transfer of personal data overseas. The approach is more permissive in respect of transfers to countries that have achieved an 'adequacy decision' from the European Commission. Australia is not on the EU's white list, unlike New Zealand, Canada, Israel, Argentina and Japan among others, which means that Australia's participation in the European market is hindered by its privacy laws. In other words, there may be pressure to reform

Australian privacy law in order to achieve an 'adequacy decision' from the European Commission and more freely participate in the European market.

The ACCC raised this as an issue in its Digital Platforms Inquiry, discussed below, as a potential benefit of enhancing privacy protection in Australia. Australia's privacy law framework was last considered for these purposes in 2001, and there were eight principal areas of concern, including the exemption of most small businesses and employee data from the scope of the Privacy Act.

## Mandatory Data Breaches Notification (MDBN) Scheme

In February 2018, roughly thirty years after the Privacy Act's commencement, it became mandatory for APP entities to notify the Privacy Commissioner and affected individuals of certain types of data breaches. Prior to this, the notification of a data breach was voluntary and rarely used.

This requirement came into effect a few months prior to the GDPR coming into effect, but well after it had been adopted in April 2016. The Australian scheme was modelled heavily on the European one, although there are some differences.

In Australia, APP entities must give notice of eligible data breaches. Eligible data breaches take place where: (a) there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by any entity; and (b) the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates. The APP entity must give notification if it has reasonable grounds to believe that an eligible data breach has happened, or it is directed to do so by the Privacy Commissioner. If unsure about whether what has happened is an eligible data breach, but there are reasonable grounds to suspect that it may have been an eligible data breach, the APP entity must carry out a reasonable and expeditious assessment of whether there are reasonable grounds to believe that an eligible data breach has taken place.

At the Privacy Commissioner's encouragement, APP entities around Australia prepared for the MDBN scheme by developing data breach response plans tailored for their organisation. According to the OAIC, in the first year of the MDBN scheme, 964 data breaches were notified, being a 712% increase on the previous twelve months under the voluntary scheme. 60% of the data breaches were malicious or criminal attacks, and 153 of the notifications were attributed to phishing. 28% of the breaches were cyber incidents where credentials were obtained by unknown means, and the vast majority of data breaches - 83% - affected fewer than 1,000 people. 35% of the notified data breaches involved human error such as unintended disclosures of personal information or the loss of a data storage device. 55% of the data breaches that occurred within the health sector, and 41% of the data breaches that occurred within the finance sector were attributed to human error (compared with 35% for all sectors). 86% of the notified breaches involved the disclosure of contact information.

Following the introduction of the Australian scheme was the implementation of the GDPR scheme in May 2018, as well as a Canadian mandatory data breach notification scheme in November 2018, and a proposal for a mandatory data breach notification scheme in New Zealand.

## OAIC

The Office of the Australian Information Commission, which houses the Privacy Commissioner, was overhauled in 2010, at the same time as the FOI system which the OAIC also administers was being revamped. Three roles were introduced at the head of the OAIC: the Information Commissioner, the Privacy Commissioner and the FOI Commissioner. In 2014, the Coalition government tried to abolish the office altogether, and almost succeeded. Its attempts were knocked back in the Senate. The OAIC's funding was so heavily cut, though, that the office in Canberra was closed and the former Commissioner was working from home.

Even with funding partly restored in 2016, the OAIC was still, according to many commentators, under-resourced. Transparency International Australia has said that the under-resourcing of the OAIC has left it on 'life support'. In March 2019, the Government announced a $25.1 million increase to the OAIC's funding over three years, which according to the current Information and Privacy Commissioner, Angelene Falk, enabled the OAIC to hire 31 more staff, boosting its head count to 124.

## Stronger privacy protection

On 24 March 2019, tougher penalties and other measures to protect Australians' privacy were announced. Once implemented, serious or repeated privacy breaches may attract increased penalties of whichever is the greater of: (a) $10 million; (b) three times the value of any benefit obtained through the misuse of the information; or (c) 10% of a company's annual domestic turnover. These penalties are still well short of those enacted by the GDPR, but bring contraventions of the privacy law in line with those of the Australian Consumer Law.

Further, the OAIC will have new infringement notice powers and other expanded options available to address breaches. Rather than having to approach the Federal Court to seek a pecuniary penalty, the OAIC would once implemented be able to use this relatively straightforward administrative remedy, in a manner similar to the ACCC and the ACMA.

Additionally, social media and online platforms will be required to stop

using or disclosing an individual's personal information on request. This would be a powerful new individual right, albeit somewhat less powerful than the right to erasure.

Moreover, there will be enhanced protection for vulnerable groups, in particular children. Lastly, the OAIC will receive significant additional funding, which did not happen when the MDBN scheme was implemented - despite the considerable additional pressure that administering the MDBN scheme would have placed on the OAIC's resources.

## Digital Platforms Inquiry

In December 2017, the ACCC began its inquiry into digital platforms - that is, search engines, social media providers and digital content aggregators - on competition in the media and advertising services markets. The inquiry was a wide-ranging exploration of the market power of digital platforms and their role in Australian society, which surveyed competition and consumer law, M&A, copyright and media regulation and the viability of journalism and the importance of media literacy in the community. But with various high-profile privacy breaches unfolding during the course of the inquiry, the focus firmly shifted to privacy regulation in Australia. One of the most noteworthy aspects of the ACCC's final report is the relatively new role for the competition and consumer regulator to play (alongside the OAIC) in protecting privacy.

The ACCC made a raft of recommendations designed to strengthen privacy protections in Australia. First, perhaps harking back to the Grubb case, the ACCC recommended that the definition of 'personal information' be amended so that it captures technical data such as IP addresses, device identifiers, location data, and any other online identifiers that may be used to identify an individual. The ACCC wants the requirements around notification and consent to be strengthened. Drawing inspiration from the European Union, the ACCC wants to see an erasure right, direct rights of action for individuals and higher penalties for breach. In addition to these changes, the Australian law should remove the exemptions for small businesses, employers and political parties. This would bring Australian law more in line with the European Union. There's yet another recommendation for a statutory tort of privacy. And the ACCC also recommends that the law require that all uses and disclosures of personal information be "fair".

That last point is an interesting one, because it makes really clear the intersection between privacy law and consumer law reflecting the author of the report.

The ACCC is naturally occupied with administering competition and consumer law. Privacy law is usually the domain of the OAIC, and communications and media law are usually the domains of the ACMA. Although privacy was not initially within the remit of the Ministerial direction commissioning the inquiry, various international developments prompted the ACCC to focus on data privacy as well. This was an interesting development in the approach to regulating personal data, because it made clear that data protection is a consumer welfare issue too.

One recommendation in particular bears that out really clearly, being the one that recommends that the *Competition and Consumer Act* be amended so that unfair contract terms are prohibited (as opposed to merely voidable, as is the current position). This would mean that there would be penalties applying to the use of unfair contract terms in any standard form consumer or small business contract. This came up in the context of the digital platform inquiry because the ACCC is concerned, in particular, with the bargains being struck between consumers and digital platforms for the collection, use and disclosure of personal data. That is, instead of looking at privacy through privacy lens only (notice, consent, reasonable expectations and so forth), the ACCC is protecting privacy by focusing on consumer issues such as unfair terms in standard form contracts between parties with bargaining power imbalances. There's an important paradigm shift there.

What practical changes will follow from the report? The Government has committed immediately to establishing a special digital platform unit in the ACCC. The Government is also setting in motion a broad review of the privacy law, and it supports most of the ACCC's recommendations in respect of privacy law changes. The Government stated that it "will commence a review of the Privacy Act to ensure it empowers consumers, protects their data and best serves the Australian economy. A review will identify any areas where consumer privacy protection can be improved, how to ensure our privacy regime operates effectively for all elements of the community and allows for innovation and growth of the digital economy. The review will also allow for further consultation on the ACCC's reform proposals to enable consumers to request the erasure of their personal information."

## What's next?

Sam Seaborn was right when he said in 1999 that the next two decades would be about privacy. And this sentiment was not at the time to be taken for granted. In the same year, Sun Microsystems CEO, Scott McNealy, famously told a group of reporters: "You have zero privacy anyway. Get over it." But with some certainty, we can say that privacy is going to continue sitting atop the regulatory agenda throughout the 20s. As Mark Zuckerberg said in 2019: "the future is private".

If the ALRC's report in 2008 set the tone for privacy reforms that came into effect in 2014, it may be fair to say that the ACCC's digital platforms

report and the inquiries that it will trigger will shape the next round of privacy reform well into the 2020s.

Putting on a pundit hat, here is some shamelessly unaccountable privacy speculation for the roaring 20s:

- With bipartisan support, the US will overcome the obstacles that had to date prevented the enactment of a comprehensive omnibus GDPR-like privacy law that applies federally and extraterritorially. Importantly, a clear, comprehensive statute will provide greater certainty to the tech companies that are subject to increasing regulatory scrutiny. Already in 2019, Mark Zuckerberg, Tim Cook and Sundar Pichai called for a comprehensive federal privacy legislation. Just as the GDPR went some way to becoming a default industry standard for data handling worldwide through its extraterritorial reach and sizeable market, the US law will drive the notion of a default industry standard even further. With GDPR-like restrictions on cross-border sharing to jurisdictions with inadequate privacy protection, other countries will look to enhance their data processing laws.
- Australia, in part motivated by a desire to trade more freely with Europe and the US, will enhance its privacy laws to bring them in line with what will increasingly become over the decade international standards. The small business and employee records exceptions will be the first to go.
- The ACCC, the eSafety Commissioner and the ACMA will join the Privacy Commissioner in the administration of data privacy in Australia. The Government's heightened appreciation for the value of data and the importance of data security will lead to stronger funding and a more holistic approach to privacy enforcement.
- With the increased application of privacy law across the Australian economy (with the removal of the small business exception), and with the increase in penalties and funding of enforcement, privacy law will become a critical compliance issue for businesses, similar to competition and consumer law.
- We will have at least four more commissioned recommendations for a privacy tort. But no tort.
- Lawmakers will struggle to find a way around the 'privacy paradox', whereby individuals purport to care about privacy but behave in ways that suggest otherwise. The well-intentioned attempts to require meaningful, informed, clear and unambiguous consent fail - because individuals don't have the capacity to grapple with each service provider's privacy policy. Instead of placing any reliance on an individual's 'consent', the Government will turn to a set of replaceable rules for data processing that effectively constitutes each entity's privacy policy. The replaceable rules become the default position, whereby entities can assume they have consent and data subjects understand the general rules of operating in the digital economy. Where a particular entity proposes to do something contrary to the replaceable rules, they are required to obtain the Privacy Commissioner's authorisation to implement such a practice and then each user's consent in relation to those items only.

# **Profile:** Associate Professor Jason Bosland

Associate Professor Jason Bosland is the Director of the Centre for Media and Communications Law at Melbourne Law School, where he teaches media and communications law. He holds degrees from the University of Melbourne and the London School of Economics. His primary research interests lie in media law, including defamation and privacy, open justice and the media, contempt of court and freedom of speech. He is an Editorial Board Member of the Media & Arts Law Review and a Research Committee Member of the Public Interest Journalism Initiative.

Associate Professor Bosland recently spoke with barrister Claire Roberts about academia, suppression orders, and what's wrong with Australian defamation law.

**CLAIRE ROBERTS:** Hi Jason, thanks for chatting with us. To kick off: how did you end up in academia, and what drew you specifically to the media law space?

**JASON BOSLAND:** I ended up in academia almost by accident. I was completing my undergraduate degree here at the University of Melbourne and I was doing some research work for some academics here in IP. And then, it just sort of happened!

I finished my LLB, then I was doing more research work and then I enrolled in a Master's. After doing that I decided that I wanted to be an academic. In terms of media law: after undertaking some research work I thought, this is really interesting. There were many IP academics at the time, but fewer people doing media law in academia so I also saw an opportunity. It's a growing area and raises all sorts of interesting issues.

**ROBERTS:** For anyone reading the *Communications Law Bulletin* who might be toying with the idea of further study – are there any broad areas of media law scholarship that are crying out for attention?

**BOSLAND:** I would say things around the national security space; government censorship; and generally I think there is a need for empirical work in the media law space. Claims are often made about the way in which media law operates to restrain journalists but this should be examined empirically.

Defamation law remains an ongoing issue in Australia; there is certainly work that needs to be done around how we reform our laws in this country. There are obviously some reforms in train – whether or not they are enough is something that could be explored. There is also a lot more work to be done around data protection. I think the questions of whether Australia should have a tort of privacy and the implications of that for privacy have been explored enough.

ROBERTS: So, defamation reform. Let's start with the serious harm threshold. Do you think it is needed? Do you think it would do anything?

**BOSLAND:** It depends on how the courts are going to interpret it. We have seen that the UK Supreme Court in *Laucaux v Independent Print* [2019] UKSC 27 has treated an equivalent provision as a real additional step that needs to be satisfied in order to bring an action.That is obviously a good development if you are thinking of ways of avoiding defamation litigation being brought. I would hope that the Australian courts will interpret it in the same way that the UK Supreme Court has.

**ROBERTS:** Do you think there are other proposed reforms that are likely to have a big impact in the defamation litigation space?

**BOSLAND:** No, probably not. Obviously the reforms around intermediaries are off the table at the moment to be dealt with at a separate time. The changes to the Contextual Truth defence probably will have an effect. That was obviously a drafting error in the existing Acts so to fix that is important. The changes to Honest Opinion might have some impact although it depends again how the courts interpret it. But I think, overall, the reforms that are currently on the table are not particularly bold. They are really focused on tinkering around the edges of the existing law.

The main problem I see with defamation law – and I think a lot of practitioners would agree with me on this – is the obsession with imputations and the idea that a plaintiff is bound to their imputations and a defendant must meet those pleaded imputations in their defences. There is very little room to argue for alternative imputations. For freedom of speech and defendants, the media in particular, that poses all sorts of problems because the plaintiff gets to set the ground rules for the entire litigation going forward. That doesn't happen in other countries. Unless we deal with some of those fundamental practice and pleading issues, some of the substantive changes may not have so much of an impact. So I think what we really need is a combination of reforming the substantive law and then also looking at the practice and procedural aspects of defamation law.

**ROBERTS:** We are speaking on the 12th of March, and as you know the High Court is hearing the Pell appeal today. It feels timely to ask: what is your view on the suppression orders in that case? Were they appropriate? Did they work?

**BOSLAND:** I am actually writing an article about this at the moment. Prominent people came out and said that this order wouldn't have been made by other judges, that Victoria doesn't have the same necessity test that exists in other jurisdictions. I think some of those comments were misguided, to be honest. Victoria *does* have a necessity test – it is there in the legislation. I don't think there is any substantive difference between the law in NSW and the law in Victoria when it comes to making these types of orders.

On the point that other judges would not have come to the same view – I think other judges would have, actually. The paper that I am writing is looking at all decisions that have been handed down where a suppression order has been granted to restrain the publication of prejudicial material in the context of back to back trials. There are very few decisions that are available – there are obviously a lot of orders made but courts usually don't issue publicly available reasons for those orders. In all of the cases I have located involving back to back trials, the orders were granted. So if you look at those decisions and you look at the circumstances in Pell – the decision in Pell is wholly consistent with those decisions – including a decision by the NSW Court of Appeal in *Nationwide News Pty Ltd v Quami* (2016) 93 NSWLR 384. So, I don't think the judge can be criticised for making the order. I think it was one that – on the current approach – was warranted.

An additional fact I suppose to be put into the mix is that it was clear from the time the order was made that the trial would almost certainly attract widespread media interest, including international media interest, and that the order would therefore be rendered futile. Now – whether that should be a factor in the judge's decision making when it comes to making this type of order is pretty controversial, actually. So you might say, well, the judge should have foreseen that the order would be ineffective because of the likelihood that there would be widespread international media attention and those international media organisations wouldn't necessarily be bound by the order. If you take that view, what you're effectively saying is that there is an expectation that someone within the jurisdiction would breach the order by conveying information to those international organisations so that they can then include that information in their publications. If a judge assumes that their order won't be followed and on that basis refuses to make it, the concern is that this has the potential to undermine the rule of law and public confidence in the courts, perhaps just as much as judges making ineffective orders. It's clearly a conundrum.

The other claim that has been made following Pell is that suppression orders are completely futile in the digital environment. In my view that argument is completely flawed. I think suppression orders are effective in 99.9% of cases; I can count on one hand the number of cases where a suppression order has been rendered futile by overseas media publishing material where an order exists. I receive and consider all the suppression orders that are sent to the media in NSW and Victoria. The ones that I think have been rendered futile or undermined by internet media publications are incredibly limited: eg, Underbelly, *DPP v Brady*, Pell.

To be clear: I don't want to be seen as apologising for the courts in making suppression orders. They do grant too many. There is definitely a problem with suppression orders in this country, but it is not around the *efficacy* of orders, I think it is around the fact that the courts make too many. The other point that I would make is that there has been a myth circulating among media for years and years that Victoria is the suppression order capital of Australia. That is absolutely not the case.

**ROBERTS:** Do you think the myth arises because Victoria reports more completely?

**BOSLAND:** Victoria and South Australia are the only two jurisdictions which send all orders made by the courts to the media. In NSW it is only the Supreme Court and sometimes the District Court – very rarely the Local Court will send out orders. Western Australia – the courts almost never sent orders out to the media. I contacted the WA Supreme Court to ask how many orders were made in recent years and the number was significant. Whereas, for example, WA made only one media notification during 2017. So, if you're relying on media notifications you're not getting a complete picture.

The other thing that needs to be factored in is caseload and population. Once you do that, surely Victoria cannot be seen as issuing orders at a greater rate per judge or capita than the WA courts.

**ROBERTS:** This is the first edition of the *Communications Law Bulletin* for 2020 and we are looking at the decades past and to come. Looking backwards over the last decade: what do you think are meaningful or important developments that we have seen, internationally or at home?

**BOSLAND:** I think the *Defamation Act 2013* in the UK was really important. We have not seen so much flow from the Leveson Inquiry in terms of substantive legal change, but I think that it promoted reflection on the conduct of the media - and that was significant. Of course, the Finkelstein Inquiry that followed in Australia did not have as much impact here as the Leveson Inquiry did in the UK.

The other big issue has probably been around data protection issues. The recent Digital Platforms Inquiry is a really important turning point in terms

of the relationship between digital platforms and traditional media organisations and consumers. This will also be very important in over the next ten years.

National security, journalists' sources and whistle-blower protection have also been very significant; in particular the mandatory data retention regime. The regime is extremely concerning when it comes to media freedom. I think that that has been wholly inadequate in terms of the measures that have been included to protect journalists' sources.

On journalists' sources more broadly: one of the major things is the privileges in the Uniform Evidence Acts. I think the way that has been interpreted in Victoria in particular has really shifted the legal landscape when it comes to journalists' sources. Interestingly, on the one hand you've got that measure which is meant to provide greater protection – and on the other hand you have a competing force which is the data retention regime, which as a practical matter means journalists are much less able to protect the confidentiality of their sources in the digital sphere.

**ROBERTS:** Now, looking forward. What do you expect to see, or not see, in the next ten years?

**BOSLAND:** I don't want to be pessimistic, but I think given history we have to be. I *don't* think we're going to see the type of reform to defamation law that I would like. I would like to see a three, four year ALRC inquiry into defamation law. Similar to what has happened in Canada: the Law Commission of Ontario has undertaken a big project on defamation law and they have basically said that anything is on the table: 'let's completely re-examine this area of law and see what we can do.' I think we need to do the same thing here. Obviously there are constitutional issues around federal legislation and things like that which would need to be ironed out – but I don't think we're going to see that sort of bold reform.

In terms of what we *are* going to see – I think we're going to see litigation involving traditional media outlets who operate on online platforms. I'm thinking particularly of the *Voller* case here – that is such a significant case, and it is so important that the Court of Appeal comes to the right decision.

**ROBERTS:** Dare I ask what the right decision is?

**BOSLAND:** The right decision is that they are not primary publishers of third party comments. For me, treating them as primary publishers of third party comments gives rise to a completely new basis for liability for publication in defamation law. They are at most secondary publishers of those comments, and if they take them down once they have notice they will be able to rely upon the innocent dissemination defence.

Returning to changes that I expect to see over the next decade: another would be I suppose – coming out of the ACCC's Digital Platforms report and the subsequent inquiry that is going on around the relationship between traditional media and online intermediaries; that's really significant as well.

Another major issue will be around data protection regimes and the liability of intermediaries when it comes to consumers. So if we treat them as media entities, which we probably should now, then I think that their responsibility will become important when it comes to things like the right to be forgotten, the use of data, transparency. If we are thinking about broad themes for the next ten years: transparency and accountability are two things that will become more important when it comes to intermediaries.

Regulation of intermediaries will also be important. For example, the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (Cth). Similarly, issues around the liability for intermediaries when it comes to the publication of 'fake news'. Singapore has introduced some legislation which hopefully is not replicated around the world because it is extremely draconian and contrary to press freedom. I think these issues can be dealt with in a much more measured way.

**ROBERTS:** Finally, the readership of the *Communications Law Bulletin* includes a lot of practitioners. Do you think that practitioners and academics engage with one another enough?

**BOSLAND:** There should be more engagement between academia and the profession – and not just those advising clients, but also the judiciary. I would like to see more empirical research based on the collection of data to come to conclusions about certain assumed things. The reverse is that academia can really benefit from the insights of practitioners. To get the perspective of what is happening 'on the ground' is very valuable for academics. I am lucky in that the Centre for Media and Communications Law has an active advisory board comprised of practitioners - I get tips and insights from them that I find really useful. Engagement amongst the profession, through events and seminars and that kind of thing, is very important as well.

**Claire Roberts,** barrister, Eight Selborne, is a member of the CAMLA Young Lawyers Committee.

# Defamation Law for a New Decade

**Sophie Dawson,** Partner (Australia), and **Phil Gwyn,** Associate (UK), Bird & Bird, discuss what lies ahead for defamation law in the new decade.[1]

## 1. Introduction

2020 and 2021 are set to be years of potentially profound change for Australia. As those of us who lack the healthcare and other skills to be of practical assistance in the current crisis make our small contribution by working from home, we contemplate the changes to society likely to be brought about not only by the rapid change in our working and living habits, but also potentially by the extensive changes being considered in relation to the laws which affect freedom of speech, civil rights and privacy issues. While our physical freedom is (hopefully temporarily) hampered by the virus, many media lawyers are hopeful that freedom of speech may be enhanced.

This article focusses on changes proposed to defamation law as part of the review of the model defamation provisions by the Council of Attorneys-General (**CAG**). The other law reform processes affecting freedom of speech which are currently on foot include the reviews of privacy law and of content laws and the various proposed codes arising from the ACCC's Digital Platforms Report in 2019. Those reforms are outside of the scope of this article.

The changes to defamation law proposed can be divided into two categories - the fundamental changes and the "fix-ups". The changes with the most potential impact are the proposed introduction of a serious harm test and the proposed single publication rule. There are also changes to the requirement that a concerns notice be issued prior to proceedings. The fix-ups include proposals aimed at changing contextual truth, statutory qualified privilege, honest opinion and jury provisions so that they achieve their original objectives.

We will deal with the fundamental changes first.

## 2. Background: The CAG Review

The last defamation law reform process seems like yesterday, but was in fact 15 years ago. In late 2004, CAG endorsed model defamation provisions. An intergovernmental agreement is in place under which there is a model defamation law working party which reports to CAG on proposals to amend defamation laws. In 2018, CAG reconvened the working party to review the model defamation provisions. In February 2019, the committee published a discussion paper and sought submissions. In December 2019, the working party published a consultation draft of proposed amendments to the model defamation provisions. Despite challenging times, there has not yet been any announcement to suggest that the reform process will deviate from the current reform timetable which anticipates the enactment of changes to the model law by the states and territories in June this year.

It has never been more important to strike the right balance when it comes to Australia's media laws. As was recognised in the ACCC's Digital Platforms Inquiry Report last year, Australian media organisations face significant challenges due to the movement of advertising dollars to digital platforms as well as globalisation and convergence more generally.

Communication laws play an important part in the competitive landscape for Australian media organisations which compete against media organisations in other places such as the US which have more media-friendly laws.

They also affect the ability and willingness of journalists and others to engage in quality journalism which the courts have repeatedly recognised is important to preserve our political and judicial systems. Overly restrictive or harsh laws might deter people from risking defamation actions in the face of shrinking advertising revenues.

This article only considers particular aspects of the proposed defamation law reforms. It focusses on how two of the reforms in question compare with their international counterparts.

## 3. The significant changes

### (a) Serious Harm

While the final form of the relevant provision is yet to be determined, with the adoption of a serious harm test in Australia, Australia will be following in the footsteps of the United Kingdom. If the current reform timetable remains on foot, within the year media lawyers will be poring over UK case authorities dealing with the serious harm test, and undoubtedly the most important of those is *Lachaux.*

Significantly, the proposed test is worded differently from its UK counterpart. This section considers the UK case law, and whether or not the differences in wording are likely to have any practical significance.

The UK serious harm test alters the test for what is defamatory and is as follows:

(1) A statement is not defamatory unless its publication has caused or is likely to cause serious harm to the reputation of the claimant.

1 With thanks to Phil Sherrell and Joel Parsons for their assistance in preparing this article.

(2) For the purposes of this section, harm to the reputation of a body that trades for profit is not "serious harm" unless it has caused or is likely to cause the body serious financial loss.

The current wording of the proposed Australian test is as follows:

(1) An individual has no cause of action for defamation in relation to the publication of defamatory matter about the individual unless the individual proves that the publication has caused, or is likely to cause, serious harm to the reputation of the individual.

(2) An excluded corporation referred to in section 9 has no cause of action for defamation in relation to the publication of defamatory matter about the corporation unless the corporation proves that the publication has caused, or is likely to cause—

  (a) serious harm to the reputation of the corporation, and

  (b) serious financial loss.

Thus, the Australian serious harm provision, if enacted, will alter the position by requiring serious harm as a prerequisite to a cause of action, but will not change the test for what is "defamatory" as has occurred in the UK.

The effect of the provision is nonetheless likely to be similar to that in the UK, as Australian Courts will no doubt look to UK authorities to apply the new provision.

***UK Case law: what does it mean for us?***

Next, we briefly consider some key UK cases. Those cases show the serious harm test can be met including in relation to social media publications. There is a question in those circumstances about the effect that the introduction of the test will have on the volume of defamation litigation in Australia, and particularly in relation to the question of whether it will reduce the large number of claims by individuals against other individuals in relation to social media publications which are currently in the Courts.

The leading UK case is the Lachaux case: *Lachaux v Independent Print Ltd & Anor* [2019] UKSC 27. In that case, the Supreme Court Justices unanimously rejected the appeal of The Independent and the Evening Standard from the High Court and Court of Appeal decision that serious harm had been caused to the claimant, Bruno Lachaux.

According to the judgment, the appellants had separately published stories detailing the divorce and subsequent custody battle between Bruno Lachaux, a French aerospace engineer, and Afsana Lachaux. The couple lived in Dubai at the relevant time, with Bruno initiating divorce proceedings in April 2011 to seek custody of their son, Louis. Afsana went into hiding, with a UAE court then awarding custody to Bruno. Mr Lachaux then found and reclaimed Louis, whilst instituting criminal proceedings against Afsana for alleged abduction.

In early 2014, the appellants published stories detailing the events described above. Bruno sued in the High Court for defamation, with the High Court deciding that the articles complained of each conveyed multiple defamatory meanings, including: that Bruno had been violent and abusive towards his wife, that he had hidden Louis' passport to prevent Afsana removing him from the UAE, that he had used UAE law and courts to deprive Afsana of custody and contact with their son, that he had callously and without justification reclaimed Louis, and that he had wrongly alleged that Afsana had abducted Louis.

In the Supreme Court, Lord Sumption delivered one of his final judgments in dismissing the appeal, which was agreed upon by the remaining four Supreme Court Justices. However, Lord Sumption differed from the Court of Appeal in his analysis of section 1(1) of the *Defamation Act 2013* (UK), thereby providing a fuller explanation of the meaning of "serious harm" within that section.

The Court concluded that the threshold of "serious harm" within section 1(1) must exceed the threshold previously established in the cases of *Jameel* and *Thornton*, and that this requirement must be applied in reference to the actual facts of the statement's impact, not just to the meaning of the words themselves.

The Court noted that the focus on the actual or likely impact of a statement is a significant departure from the common law. At common law, damage is conclusively presumed once defamatory meaning is established.

Key common law principles were nonetheless applied when applying this test. They included:

(a) The "repetition rule", to the effect that "a statement that someone else has made a defamatory statement about the claimant, although literally true, is treated as equivalent to a direct statement to the same effect. The policy is that "repeating someone else's libellous statement is just as bad as making the statement directly": *Lewis v Daily Telegraph* [1964] AC 234, 260 (Lord Reid)": *Lachaux* at paragraph 23; and

(b) the *Dingle* rule (see *Associated Newspapers Ltd v Dingle* [1964] AC 371), the effect of which, in Lord Sumption's words, is "to treat evidence of damage to the claimant's reputation done by earlier publications of the same matter as legally irrelevant to the question what damage was done by the particular publication complained of": at paragraph 24.

It will be interesting to see whether the same approach will be taken to the Australian test in circumstances in which it seems likely to separate

the serious harm requirement from the test for what is defamatory. Australian courts will need to decide how much of the existing case law concerning defamatory meaning to carry across to the new provision.

It is instructive to consider the approach taken in that case to establishing serious harm, which provides some guidance as to the types of evidence which are likely to be put on in defamation cases after the test is introduced. Lord Sumption's description of the evidence is as follows:

> "On the footing that (as I would hold) Mr Lachaux must demonstrate as a fact that the harm caused by the publications complained of was serious, Warby J held that it was. He heard evidence from Mr Lachaux himself and three other witnesses of fact, and received written evidence from his solicitor. He also received agreed figures, some of them estimates, of the print runs and estimated readership of the publications complained of and the user numbers for online publications. He based his finding of serious harm on (i) the scale of the publications; (ii) the fact that the statements complained of had come to the attention of at least one identifiable person in the United Kingdom who knew Mr Lachaux and (iii) that they were likely to have come to the attention of others who either knew him or would come to know him in future; and (iv) the gravity of the statements themselves, according to the meaning attributed to them by Sir David Eady. Mr Lachaux would have been entitled to produce evidence from those who had read the statements about its impact on them. But I do not accept, any more than the judge did, that his case must necessarily fail for want of such evidence. The judge's finding was based on a combination of the meaning of the words, the situation of Mr Lachaux, the circumstances of publication and the inherent probabilities. There is no reason why inferences of fact as to the seriousness of the harm done to Mr Lachaux's reputation should not be drawn from considerations of this kind. Warby J's task was to evaluate the material before him, and arrive at a conclusion on an issue on which precision will rarely be possible. A concurrent assessment of the facts was made by the Court of Appeal. Findings of this kind would only rarely be disturbed by this court, in the absence of some error of principle potentially critical to the outcome."

The finding that actual harm is relevant to the serious harm test has practical implications. It means that, in principle at least, a statement which is not defamatory (in the UK) or which is defamatory but not actionable (in Australia) due to lack of serious harm may become defamatory (UK) or actionable (in Australia) if it later results in serious harm.

### *How will the serious harm test affect social media cases?*

The UK case law also establishes that, whilst the serious harm test may dispose of many of the social media and other online "backyarders" currently clogging up the court system, some online publications will still be actionable. The case of *Monroe v Hopkins* related to the defacement of the Memorial to the Women of WWII in Whitehall during an anti-austerity demonstration on Saturday 9 May 2015. Amongst widespread media condemnation, on 9 May the New Statesman journalist Laurie Penny tweeted under the Twitter handle @PennyRed that "I don't have a problem with this. The bravery of past generations does not oblige us to be cowed today."

In what was accepted to be a case of mistaken identity, on 18 May Ms Hopkins posted a tweet to Ms Monroe, asking:

> "scrawled on any memorials recently? Vandalised the memory of those who fought for your freedom. Grandma got any more medals?"

Following Ms Monroe's clarifications that she hadn't been involved, Ms Hopkins deleted the first tweet, replacing it with:

> "can someone explain to me – in 10 words or less – the difference between irritant @PennyRed and social anthrax @MsJackMonroe"

Following continued mud-slinging on Twitter, on 2 June Ms Hopkins tweeted: "@MsJackMonroe I was confused about identity. I got it wrong." But demands from Ms Monroe for an apology and a donation to charity were not met by Ms Hopkins, so proceedings were issued by Ms Monroe in December 2015.

As Mr Justice Warby identified in his opening remarks on 10 March 2017, the three central points in issue were: (1) the meaning of the two tweets; (2) whether these tweets amounted to defamation; and (3) whether they had caused or were likely to cause serious harm to Ms Monroe's reputation.

### *What did the tweets mean?*

Mr Justice Warby ruled that the meaning of the first tweet was not literal, as the hypothetically reasonable readers of Ms Hopkins' Twitter feed would not believe that Ms Monroe had literally vandalised the war monument herself. However, the ordinary and natural meaning in the eyes of the reasonable reader was that Ms Monroe "condoned and approved of the fact that in the course of an anti-government protest there had been vandalisation by obscene graffiti of the women's war memorial in Whitehall, a monument to those who fought for her freedom."

In discerning the meaning of the second tweet, the judge found that when read in the context of the first tweet, the second tweet carried the innuendo meaning that Ms

Monroe condoned and approved of the defacing of the women's war memorial, despite the fact that the first tweet had been deleted by the time that the second tweet was published. In making this finding, the judge noted that the two should be read together as the first tweet had been published only shortly beforehand. Simply deleting a tweet is not a satisfactory defence to a libel claim.

***Were the tweets defamatory?***

In order to establish a claim in defamation, Ms Monroe's lawyers had to show that the meaning of the tweets would tend to have a substantially adverse effect on the way that right-thinking members of society generally would treat Ms Monroe.

Anticipating charges (subsequently made) that his decision would be portrayed by Ms Hopkins and her supporters as tantamount to an attack on freedom of speech, Mr Justice Warby emphasised that "the demands of pluralism in a democratic society make it important to allow room for differing views to be expressed without fear of paying damages for defamation. Hence, a statement is not defamatory if it would only tend to have an adverse effect on the attitudes to the claimant of a certain section of society."

With that said, Mr Justice Warby had no difficulty in deciding that the meaning of Ms Hopkins' tweets was defamatory as they would lower Ms Monroe in the estimation of "right-thinking people generally". In support of this conclusion, Mr Justice Warby simply stated that defacing a public monument is a crime, and that society as a whole would view both illegal acts and showing disrespect to those who gave their lives in World War II as deplorable.

***Was serious harm established?***

On the serious harm question, Mr Justice Warby found that "the tweets complained of have a tendency to cause harm to this claimant's reputation in the eyes of third parties, of a kind that would be serious for her."

Amongst the factors influencing the judge on this point was the extent of the tweets' publication on Twitter. Ms Hopkins' argument was that as the first tweet was an 'at reply' tweet (i.e. a tweet which begins with the Twitter handle of the recipient), only Twitter users who followed both Ms Hopkins and Ms Monroe would have received this tweet, a number that the defence estimated at just 140. Notwithstanding this fact, the judge decided that the probable audience to the tweet was in the region of 20,000. In deciding this, the judge considered that the tweet was available on Ms Hopkins' home page for 2 hours and 25 minutes, and that as Ms Hopkins received 5.74m direct profile views in May 2015, this time period equates to roughly 25,000 impressions. Although this figure is not exact as not all those Twitter users to whom the tweet was accessible will have actually read it, given that potential impressions do not take into account views through retweets, an audience of 20,000 was decided as an acceptable estimate.

Ms Hopkins' lawyers also sought to defend her by arguing that she was simply an unauthoritative voice in the "Wild West" of social media and her remarks could therefore not possibly cause serious harm to somebody's reputation. This argument was rejected by Mr Justice Warby, who noted that Ms Hopkins was a "well-known figure" and that she was a newspaper columnist for the Sun at the time.

Finally, Ms Hopkins' lawyers argued that serious harm could not be established due to her tweet of 2 June 2015 admitting that a mistake had been made. However, just as the first tweet was an 'at reply' tweet, and would only arrive on the timelines of their 140 mutual followers, so was the tweet admitting Ms Hopkins' error. Furthermore, Mr Justice Warby found that this tweet was unsatisfactory as an apology because of four key factors: (a) it was several weeks after the event; (b) it was early in the morning, at a time when tweet impressions are lower; (c) it was not self-explanatory; and (d) it carried no apology.

The judge's comments have implications for social media defamation claims in both the detailed methodology used to discern the extent of publication and the rejection of the idea that certain users of Twitter are not authoritative sources who can cause serious harm to reputation by their comments. If comments are made in error, Mr Justice Warby's judgment makes it clear that a swift, conspicuous and clear apology is the most effective way to minimise the risk of claims. Indeed, in his closing remarks he also made it clear that the case could have easily been resolved if an open offer to settle for £5,000 had been accepted.

Additionally, the judge observed that a difficultly arose because the first tweet had been deleted and that Twitter Analytics (a tool used to measure a user's impact on Twitter) was therefore unavailable to accurately determine the scale of its distribution. He also highlighted that many supposedly abusive tweets to Ms Monroe were automatically deleted by a piece of software which she used to remove offensive and threatening tweets from 'trolls'. As he highlighted, it is "the responsibility of a litigant to retain and preserve material that may become disclosable," and the responsibility of a solicitor to ensure that their client appreciates this.

It is proposed in Australia that the defence of triviality be removed as part of the reform package. This is a natural corollary of introducing the serious harm test: If the defence were to remain, this could cause the serious harm test to be read down.

## (b) Single Publication Rule

The second most significant reform proposed is the introduction of a "single publication rule" in Australia.

At the moment, much news and other potentially defamatory material is published either in mass media publications, or online.

In 2002 the High Court confirmed in the *Gutnick* case that the multiple publication rule applies. The effect of this is that a new cause of action arises each time a defamatory communication is received by a new person. Moreover, the Court in *Gutnick* also confirmed that the place of each defamatory publication is the place of the recipient, and that the applicable law is that of the recipient, with the result that a single internet publication can rapidly give rise to causes of action under different laws and at different times across the world. Moreover it can continue to give rise to such causes of action indefinitely.

The choice of law aspects of the *Gutnick* decision were partially addressed by the ch0ice of law provisions in the Uniform Laws introduced in Australia in 2005. Those laws stipulate that within Australia the applicable law is that of the place with the closest connection with the harm. The substantial uniformity of Australian laws also makes choice of law less important within our borders. Interestingly, that law reform did not remedy the international choice of law position, but that does not seem to have resulted in any major practical problems.

The reform now being considered will address the limitation period aspects of the multiple publication rule. These were most famously illustrated by the Duke of Brunswick when he sent his manservant down to buy a back issue of a newspaper so that he could sue on publication of the back issue to his manservant after the limitation period expired: *Brunswick v Harmer* (1849) 14 QB 185, [1849] EngR 915, (1849) 117 ER 75.

The "single publication rule" title is taken from the US single publication rule. The proposed statutory amendment only picks up one aspect of that US rule. The US single publication rule was summarised in *Gutnick*[2] as follows:

> "Some 27 States of the United States, including California, Illinois, New York, Pennsylvania and Texas, by legislation or by judicial decision have adopted what is identified as the single publication rule. That rule is set out in §577A of the *Restatement of Torts*, 2d, (1977), which is headed "Single and Multiple Publications", and reads:
>
> "(1) Except as stated in Subsections (2) and (3), each of several communications to a third person by the same defamer is a separate publication.
>
> (2) A single communication heard at the same time by two or more third persons is a single publication.
>
> (3) Any one edition of a book or newspaper, or any one radio or television broadcast, exhibition of a motion picture or similar aggregate communication is a single publication.
>
> (4) As to any single publication,
>
> (a) only one action for damages can be maintained;
>
> (b) all damages suffered in all jurisdictions can be recovered in the one action; and
>
> (c) a judgment for or against the plaintiff upon the merits of any action for damages bars any other action for damages between the same parties in all jurisdictions."
>
> In *Firth v State of New York*, the New York Court of Appeals decided that the one-year statute of limitation in New York runs from the first posting of defamatory matter upon an Internet site and that the single publication rule applies to that first posting."

The proposed Australian provision is as follows:

**1A Single publication rule**

(1) This section applies if—

(a) a person (the ***original publisher***) publishes matter to the public that is alleged to be defamatory (the ***first publication***), and

(b) the original publisher or an associate of the original publisher subsequently publishes (whether or not to the public) matter that is substantially the same.

(2) Any cause of action for defamation against the original publisher or an associate of the original publisher in respect of the subsequent publication is to be treated as having accrued on the day of the first publication for the purposes of determining when—

(a) the limitation period applicable under section 1 begins, or

(b) the 3-year period referred to in section 1B(2) begins.

(3) Subsection (2) does not apply in relation to the subsequent publication if the manner of that publication is materially different from the manner of the first publication.

(4) In determining whether the manner of a subsequent publication is materially different from the manner of the first publication, the considerations to which the court may have regard include (but are not limited to)—

(a) the level of prominence that a matter is given, and

(b) the extent of the subsequent publication.

2 *Dow Jones & Company Inc v Gutnick* [2002] HCA 56; 210 CLR 575; 77 ALJR 255; 194 ALR 433 Per Gleeson, McHugh, Gummow & Hayne JJ .

(5) This section does not limit the power of a court under section 1B to extend the limitation period applicable under section 1.

***associate*** of an original publisher means—

(a) an employee of the publisher, or

(b) a person publishing matter as a contractor of the publisher, or

(c) an associated entity (within the meaning of the *Corporations Act 2001* of the Commonwealth) of the publisher.

***day of first publication***, in relation to publication of matter on a website or in any other electronic form, means the day on which the matter was first posted or uploaded on the website or sent electronically.

***public*** includes a section of the public.

The wording of this provision is likely to give rise to difficult questions as to when publications are relevantly "substantially" the same and when differences in the "manner" of publication are sufficient for there to be separate limitation periods where proceedings have previously been brought against the same defendant or an associate of the same defendant.

A new proposed section 23 will address the potential for multiple actions in relation to the same or like matter in Australia. It provides that leave of the court is required to bring an action in respect of matter which is the same as or like matter in relation to which proceedings have previously been brought against the same defendant or an associate of that defendant.

## 4. The Fix Ups

The fix ups are largely uncontroversial amongst defamation lawyers. There are clear changes required to meet the objectives of aspects of the Uniform Acts as originally drafted.

*1.1 Requirement for a concerns notice*

The amendments will require plaintiffs to serve a concerns notice on each defendant and to wait at least 14 days before suing.

This will enhance the settlement opportunities in relation to potential claims, and will open the door for potential defendants to make offers under the offer of amends provision. A number of tidy ups have been made to the offer of amends provisions as part of the proposed reforms, including a requirement for offers to be open for at least 28 days.

*1.2 Contextual Truth*

Amendments have been proposed which address the *Kermode* problem in relation to existing contextual truth defences[3]. Due to a drafting issue in relation to existing contextual truth defences, plaintiffs have been able to defeat the contextual truth defence by "pleading back" imputations relied on as contextual truth imputations.

The amendment addresses this by making it clear that imputations pleaded by a plaintiff can be relied upon as contextual imputations by a defendant.

*1.3 The Zunter Problem*

The statutory qualified privilege defence in the Uniform Law was designed to attract the UK *Reynolds* case law.[4] Unfortunately, the Courts interpreted the defence as imposing a very high bar of reasonableness, particularly in *John Fairfax Publications Pty Ltd v Zunter* [2006] NSWCA 227.

The reforms address this with a new section 29A which introduces a defence of responsible publications in the public interest. They also make important adjustments to the existing statutory qualified privilege defence in section 30 to make the availability of the defence a matter for juries rather than judges, and to make it clear that the list of matters in that section (which were taken from *Reynolds* in the last round of amendments) are not comprehensive and do not all need to be taken into account.

*1.4 Aggravated damages and the cap*

Amendments to the limit on damages for economic loss make it clear that the maximum must only be awarded in a most serious case.

However, they also broaden the potential for aggravated damages awards by removing the previous limited provision for aggravated damages and replacing it with a broad provision allowing the award of aggravated damages where they are "warranted in the circumstances".

## 5. Conclusion

If enacted, the reforms to defamation laws could have a significant effect on defamation practice in Australia. The serious harm text and the single publication rule in particular could stem the flow of internet-related small claims currently clogging the Court system. Much will, however, depend on how the Courts interpret each of the new provisions. Overseas case law provides some guidance but the unique drafting of the proposed provisions will also give Australian Courts latitude to interpret them differently.

3 *Fairfax Media Publications Pty Ltd and Others v Kermode* [2011] NSWCA 174

4 *Reynolds v Times Newspapers Ltd* [2001] 2 AC 127

# A Decade of Contempt and the Media:
## Ensuring That Justice Must Be Seen to be Done

**Katherine Giles,** Senior Associate at MinterEllison, discusses the previous decade in contempt law and where the 20s might take us.

> *'... the principle of open justice – is one of the most pervasive axioms of the administration of justice in our legal system. It informs and energises the most fundamental aspects of our procedure and is the origin, in whole or in part, of numerous substantive rules.'*[1]

In the last decade, media organisations in Australia have played a crucial role in promoting and protecting open justice. Underpinning the law of contempt is the broad notion that justice should be open, and must be seen to be done. It is media organisations that largely assume responsibility for presenting arguments to the court as to why a court should remain open, or why it should not suppress the publication of information, when applications are made to a court to sit in camera or to issue non-publication or suppression orders. In playing this role, media organisations are required to put forward open justice arguments, and a contention that the public have the right to know what transpires in the courts.

The benefits of open justice include providing a check on the veracity of witnesses, benefits to litigants looking for public vindication, community legal education, reducing the likelihood of uninformed and inaccurate commentary about court cases, reassuring the public that justice is administered fairly, impartially and in accordance with the rule of law, and preventing the exercise of arbitrary power by judges. Balanced against this are the costs of open justice. These costs include the loss of privacy and reputation, media focus, embarrassment, distress, shame and financial harm to those involved.[2]

It can also include threats to personal and national security.

Debates surrounding the benefits and costs, and the general rule underpinning the law of contempt may have developed over many centuries.[3] However, the last decade has rendered this concept subject to changes in the media landscape, the pervasive access to social media, and the user generated content and media cycle that comes with it. As my colleagues Peter Bartlett and Tess McGuire recently noted:

> *'Our society has adapted and embraced the vast change that social media and technology have caused, but our media laws have not. The limited ability of our defamation and suppression order regimes to respond to the disruption has received much attention over the past year. Action is needed. Not mere tinkering at the edges, but reform that seeks to restore a balance between protecting reputations and freedom of speech.'*[4]

Media contempt can take the form of a breach of contempt in the face of the court, sub judice contempt, breach of suppression order, scandalising the court, breaching jury secrecy, and disobedience of court orders or disrupting the court for example, using cameras or sound recording equipment in court or refusing to answers questions or follow directions in court. The fundamental objective of the law of contempt is providing a fair trial, ensuring compliance with the courts orders and protecting the administration of justice. However, the media also have an important role to play in upholding and protecting these objectives, and the impact on media freedoms is balanced with the proper administration of justice, and the rights and legitimate expectations of individuals involved in legal proceedings. The media act as a surrogate for the public, and the courts facilitate media access to the courts.[5] Given the impact on media freedom, it is not surprising that these laws are routinely criticised, and over the last decade have been the subject of numerous enquiries and reports.

In the last decade a number of decisions demonstrate the role of the media in ensuring that justice must be seen to be done. In *News Digital Media Pty Ltd v Mokbel* (2010) 30 VR 248 Warren CJ and Bryne J noted the tension between open justice and the administration of justice, but indicated that an interest in Mokbel did not *'rank*

1 The Honourable JJ Spieglman, 'Seen to be Done: The Principle of Open Justice' – Pt I' (2000) 74 *Australian Law Journal* 290 (Pt II at 378), 292.

2 The Right Honourable Beverley McLachlin --- 'Courts, Transparency and Public Confidence - To the Better Administration of Justice' [2003] DeakinLawRw 1; (2003) 8(1) Deakin Law Review 1.

3 C J Miller and David Perry, *Miller on Contempt of Court* (Oxford University Press, 4th ed, 2017) 2.

4 Peter Bartlett and Tess McGuire, 'The year in Australian media law', *Medium* (May, 2019) available at https://pressfreedom.org.au/the-year-in-australian-media-law-3163135f4fdc?gi=ba2b5c8c5c05

5 Hon Chief Justice Marilyn Warren, 'Open Justice in the Technological Age' (2014) 40(1) *Monash University Law Review* 45; Jason Bosland, 'Two Years of Suppression under the *Open Courts Act 2013* (Vic)' (2017) 39(1) *Sydney Law Review* 25.

*at the highest level of principle.'* Despite this, 24 non-publication orders were issued supressing the publication of Mokbel's prior convictions, charges against him and associations with other people involved in the Melbourne gangland war. The court also ordered that all media organisations remove all articles about Mokbel from the internet. The suppression orders were lifted when Mokbel later entered a guilty plea in relation to the drug trafficking charges in 2011. In contrast, in *Fairfax Digital Australia and New Zealand Pty Ltd v Ibrahim* (2012) 83 NSWLR 52 in which Bennett DCJ made orders purporting to operate throughout Australia during criminal proceedings involving Fadi and Michael Ibrahim and Rodney Atkinson, who were facing prosecution in the District Court of New South Wales on a number of charges. The orders prohibited any disclosure, dissemination or provision of access, by book, newspaper, magazine, radio or television broadcast or on the internet of any criminal proceedings involving the Ibrahims or Atkinson as parties or witnesses, material referring to other alleged unlawful conduct involving the Ibrahims or Atkinson, and conduct they were suspected of being complicit in or having knowledge of. Eight media companies challenged the validity of the orders in the New South Wales Court of Criminal Appeal. The court held that the order was an *'overreach'* and that '*the scope of the order is inherently suspect to the extent that it seeks to prevent the whole population of Australia having access to the offending material, at least for a period, in order to prevent possible access by a juror or member of the jury panel for a particular case.'* The court also held that orders must be necessary to avert an interference in the course of justice, and cannot be merely *'convenient, reasonable or sensible… or that would serve some notion of the public interest'*. Further to this, the court held that *'an order will fail the necessity test if it is futile… [a]s a matter of construction, that which is ineffective cannot be described as "necessary"'*. In addition, there was a concern that the orders would have an impact on ISPs and search engines. Accordingly, the orders made by Bennett DCJ were held to be ineffective and therefore not necessary, and as they did not satisfy the grounds of section 8(1)(a) of the *Court and Suppression and Non-publication Orders Act 2010* (NSW), they should not have been made.

Following *DPP (Cth) v Besim; DPP (Cth) v MHK (No 2)* [2017] VSCA 165, in June 2017 *The Australian* published the article *'Judiciary 'Light on Terrorism'*, including comments from Minister Greg Hunt, Alan Trudge and Assistant Minister Michael Sukkar criticising the judiciary whilst the judgments in *Besim* and *MHK* were reserved. The Judicial Registrar of the Court of Appeal sent letters to the Attorney-General with respect to the ministers, the publisher, editor and journalist who authored the article. The Court of Appeal convened a mention in both cases and the parties were all present in the court during which the parties all offered apologies, and the court accepted the apologies and stated that they would not refer the parties for contempt of court. Warren CJ observed that the comments were *'fundamentally wrong'* and that the delay in apologising was *'regrettable and aggravated the contempt'*, and went on further to state:

> *'Given that the court's decisions in both cases were pending, the court is concerned that the attributed statements were impermissible at law and improperly made in an attempt to influence the court in its decision or decisions. Further, the court is concerned that some of the statements purported to scandalise the court. That is by being calculated to improperly undermine public confidence in the administration of justice in this state in respect of the disposition of the appeals that the court has presently under consideration.*
>
> *The court was further concerned that the attributed statements were made by three ministers of the Crown. The statements on their face:*
>
> - *fail to respect the doctrine of separation of powers;*
> - *breach the principle of sub judice; and*
> - *reflect a lack of proper understanding of the importance to our democracy of the independence of the judiciary from the political arms of government.'*

Most importantly the court noted that the parties should comprehend that the court hasn't been, and will not be affected by the statements made in The Australian, or elsewhere in the media. Noting further to this, that the parties should be assured that an article will not have an effect on the decision or decisions the court will make, and that the court will be independent, impartial and in accordance with the rule of law. No contempt charges were laid, and this is not a decision that involved the media. Nonetheless, it highlights the importance the court will place on upholding the legal notions of contempt of court, and emphasising that they do not exist to protect judges or their personal reputations, but rather to protect the independence of the judiciary that bind both governments and decisions, and instill public confidence in the judiciary.

There have also been a number of reports and reviews considering contempt law.[6] All of these

6 See The Report of the Australian Law Reform Commission (ALRC), *Contempt* (June, 1987); NSW Law Reform Commission (NSWLRC), Discussion Paper 43, *Contempt by Publication* (July 2000); NSWLRC, Discussion Paper 100, *Contempt by Publication* (June, 2003), Australia's Right to Know, *Report of the Review of Suppression Orders and Media's Access to Court Documents and Information* (November, 2008).

recognise that there is a need to clarify the role of the media and the balance between open justice and the administration of justice. Most recently, on 15 August 2017 the Senate referred a number of issues to the Constitutional Affairs References Committee for inquiry and report by 25 November 2017, with the submissions to be referred to any future Senate inquiry into contempt. These included a consideration of a number of previous recommendations including that:

- the common law principles be abolished and replaced by statutory provisions – arising from the Australian Law Reform Commission (**ALRC**) report in 1987;
- the need to achieve clarity and precision in the operation of the law on sub judice contempt (arising from the NSWLRC report in 2003);
- the development and operation of statutory provisions in Australia and overseas that codify common law principles of contempt; and
- the importance of balancing principles, including freedom of speech and expression, the right of fair trial by an impartial tribunal, public scrutiny of the operations of the court system and the protection of the authority, reputation and due process of the courts.

The views of submitters were mixed, particularly in relation to whether the law of contempt should be codified, and the committee recommended that the submissions received to the inquiry be referred to any future Senate inquiry into contempt.[7]

In October 2018, the Victorian Law Reform Commission (**VLRC**) was asked to review and report on the law relating to contempt of court, the possible reform of the *Judicial Proceedings Report Act 1958* (Vic), and the legal framework for enforcement of prohibitions or restrictions on the publication of information and all types of contempt law. In 2019, the VLRC launched the review of contempt laws in Victoria. The launch followed public debate about the use of suppression orders, to consider whether jurors and court officers need to be educated about social media, and whether messages about court proceedings sent to groups through private messages through social media should be considered as a breach of a suppression or non-publication order. This review was ordered by the Attorney General in December 2019, after a jury delivered a unanimous guilty verdict in the trial of Cardinal George Pell for historic child sexual abuse offences. And was further propelled by the multiple charges brought by the Victorian Director of Public Prosecutions, Kerri Judd QC against 36 journalists and media organisations following the publication of headlines and other publications when Cardinal George Pell was convicted in December 2018. A key concern for the Commission, and a theme running through the consultation paper, is *'the lack of certainty and clarity in the common law of contempt of court, and the effect that uncertainty on the proper and effective administration of justice and public confidence in the work of the courts."*[8]

In February 2019, the Law Council of Australia called for an ALRC review of suppression orders and uniformity across jurisdictions.[9] Law Council President, Arthur Moses SC, stated that: *'At its core, this issue involves striking the right balance between open justice including the public interest in court reporting, and the right of the individual to a fair trial.'* He also noted that Australian journalists *'are amongst the best trained and respected in the world and informed reporting of our legal system maintains public confidence in the judiciary and the courts.'* In early 2019 the NSW Attorney-General Mark Speakman also asked the NSW Law Reform Commission to consider whether the laws around suppression and non-publication orders had the balance right. Preliminary submissions to the open justice review closed on 31 May 2019. And in January 2020, the Tasmania Law Reform Institute considered contempt law, jurors, social media and the right of an accused to a fair trial.[10] The Institute recommended that changes to the law are not necessary, and the preferred strategy to address juror misconduct is updating and improving juror pre-empanelment training, resources and education, and the introduction of model jury directions.

There have also been recent calls to introduce a Media Freedom Act that would recognise and affirm the importance of press freedoms, and attempt to balance open justice and the administration of justice, to ensure that justice continues to be seen to be done.

**Katherine Giles** is a Senior Associate at MinterEllison specialising in intellectual property, entertainment and media law, and prior to this was a Senior Lawyer at the ABC. She is also the Treasurer of CAMLA, an active Arts Law Centre of Australia volunteer, and a teaching fellow in the Law Faculty at the University of New South Wales.

7 Submissions were received by the Legal Services Commission of South Australia, Law Council of Australia, Office of the Director of Public Prosecutions (NSW), International Commission of Jurists Victoria, Ms Melville Miranda and Mr Dominic Kanak.

8 Victorian Law Reform Commission, *Contempt of Court: Consultation Paper* (2019) [2.42].

9 https://www.lawcouncil.asn.au/media/media-releases/law-council-calls-for-alrc-review-of-suppression-orders-uniformity-across-jurisdictions

10 Tasmania Law Reform Institute (**TLRI**), Final Report No. 30, *Jurors, Social Media and the Right of an Accused to a Fair Trial* (January 2020).

# All Talk, No Cause of Action:

## Where to Next for an Australian Cause of Action for Serious Invasion of Privacy?

**Jim Micallef** and **Madeleine James** at Corrs Chambers Westgarth discuss the developments that took place in the 2010s in relation to a privacy tort in Australia, and what may lie ahead in the 2020s.

In a report considering the adequacy of Australian privacy laws in the context of rapid developments in technology, the Australian Law Reform Commission made the following comments on the need for a cause of action for invasion of privacy:

> *In Australia, the number of privacy-invading publications appears to be small. No doubt most journalists are sensitive to privacy issues. Lapses occur infrequently but this is inconclusive. Many laws are [infrequently] breached but they are enacted and maintained to set community standards. In at least some cases, significant harm has been done by a deliberate intrusion not justified by any public purpose… The consequences of invasion have, in some cases, been quite devastating. From the victim's point of view the effect, not frequency, is the critical matter. The delivery to an offender of a mere reprimand, by a conciliation body such as a Privacy Committee or a Press Council, appears to be an inadequate redress for a wronged person. The possibility of a reprimand has not been shown to be an effective deterrent to privacy-invading publishers.*[1]

It is telling of the progress that has been made in this space that this statement was not part of the ALRC's 2014 report, *Serious Invasions of Privacy in the Digital Era*, but rather its 1979 report *Unfair Publication: Defamation and Privacy*. The last several decades, and in particular the 2010s, have seen a series of successive law reform commission reports and parliamentary inquiries, always leading to the same conclusions: that Australian law offers no solution to an individual who suffers a serious, unjustified invasion of privacy, and that it ought to. However, no statutory cause of action has been introduced. In the courts, there has been a similar lack of progress, with some lower courts awarding damages on the basis of a common law cause of action, but to date, no recognition by an appellate court of a tort of invasion of privacy.

In recent times, talk of introducing a statutory cause of action for invasion of privacy has been swept up into conversations about the protection of personal information and data security. Leaving aside data privacy concerns, despite repeated recognition of the need for a cause of action for invasion of privacy, a gap remains for those persons whose private lives are, without their consent, thrust into the public sphere, but for whom a cause of action in defamation is doomed to fail against a defence of truth. Looking forward, the question of a tort of invasion of privacy will once again be the subject of a government review, according to the Commonwealth Government's response to the ACCC's *Digital Platforms Inquiry Final Report* released last year.

### A decade of inaction

The last decade in particular has been marked by repeated recommendations for a model based on essentially the same principles underpinning the ALRC's recommendations in 1979.

In 2009, the NSW Law Reform Commission concluded that the introduction of a general cause of action for invasion of privacy would both fill gaps in existing law, and recognise the inherent value of privacy "*in a climate of dynamic societal and technological change*."[2] The following year, the Victorian Law Reform Commission recommended the introduction of two statutory causes of action for invasion of privacy, separated into the misuse of private information and intrusion upon seclusion.[3] An issues paper by the Department of the Prime Minister and Cabinet in 2011 acknowledged that a cause of action for invasion of privacy would not only address emerging challenges posed by mobile technology, cloud computing, and the rise of social media and video sharing websites, but would also provide an additional mechanism for the promotion of privacy in accordance with Australia's obligations as a party to the International Covenant on Civil and Political Rights.[4]

1 Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy* (Report No. 11, 1979), [230].

2 New South Wales Law Reform Commission, *Invasion of Privacy* (Report No. 120, April 2009), [4.14].

3 Victorian Law Reform Commission, *Surveillance in Public Places* (Report No. 18, June 2010).

4 Department of the Prime Minister and Cabinet, 'Issues Paper: A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy' (September 2011).

Perhaps the most comprehensive analysis of this area was undertaken in 2014 by the ALRC.[5] Its report, *Serious Invasions of Privacy in the Digital Era*, echoed the recommendation made in its 2008 report on privacy law,[6] while diving deeper into the precise manner in which the cause of action should be implemented and detailing the proposed elements for a statutory cause of action in tort to be enacted in a new Commonwealth statute. The report was tabled in parliament in September 2014, but was doomed to be ignored: the Attorney-General had issued a statement months earlier advising that the government would not support a tort of privacy. An inquiry by the NSW Parliament Standing Committee on Law and Justice in 2016 also did not prompt legislative reform.[7]

At the tail end of the decade, the ACCC recommended in its Digital Platforms Inquiry Final Report that a new statutory cause of action be created to cover serious invasions of privacy. The statutory cause of action contemplated by the ACCC would provide a remedy for either misuse of private information or intrusion upon seclusion, provided a certain standard of seriousness was satisfied – fundamentally the same model recommended by the ALRC in 2014.

From a common law perspective, there has been a similar lack of progress. Several lower court decisions have recognised the existence of a cause of action based on invasion of the claimant's privacy.[8] The first of these decisions, a decision of the Queensland District Court in 2003, labelled it as a "*logical and desirable step*", albeit a bold one, to recognise an actionable right to privacy for the first time. However, those cases were settled before appeals could be heard, eliminating an opportunity for an intermediate court of record to decide the issue.

Essentially, no real progress has been made other than to reiterate the High Court's acknowledgment in *Australian Broadcasting Corporation v Lenah Games Meats* that an actionable right for invasion of privacy may be available to individuals, albeit not one grounded in tort:

> *…Lenah's reliance upon an emergent tort of invasion of privacy is misplaced. Whatever development may take place in that field will be to the benefit of natural, not artificial, persons. It may be that development is best achieved by looking across the range of already established legal and equitable wrongs. On the other hand, in some respects these may be seen as representing species of a genus, being a principle protecting the interests of the individual in leading, to some reasonable extent, a secluded and private life. … Nothing in these reasons should be understood as foreclosing any such debate or as indicating any particular outcome.*[9]

## Lagging behind foreign jurisdictions

While little progress has been made in Australia, comparable jurisdictions have surged ahead in recognising actionable privacy rights.

In the United Kingdom, a cause of action has been confirmed to exist by virtue of the ratification of the European Convention of Human Rights, through the introduction of the *Human Rights Act 1998* (UK). Within a few years, the House of Lords had recognised that the combination of enshrined rights created an actionable tort, provided there was a legitimate expectation of privacy on the part of the claimant, in relation to the information that was disseminated, and the absence of justification on the part of the respondent, in that its breach of the claimant's legitimate expectation of privacy was not vindicated by virtue of a right to freedom of expression. Numerous high profile cases have been brought in recent years.[10] It remains to be seen how this area of law will be affected by Brexit.

In New Zealand, a common law tort of invasion of privacy, based on misuse of private information, was first recognised by the Court of Appeal in 2005.[11] The tort had two fundamental requirements: the existence of facts in respect of which a reasonable expectation of privacy existed, and that the publicity given to those private facts would be considered highly offensive to an objective person. Freedom of expression is accommodated through the availability of a public interest defence, and in the sense that the remedy available was damages, rather than injunctive relief. A further form of the tort based on intrusion upon seclusion was subsequently recognised by the High Court in 2012, introducing the additional requirements of an intentional and unauthorised intrusion, into 'seclusion' (such as the claimant's intimate personal activities, space or affairs).[12]

5 Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Report No. 123, July 2014).

6 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No. 108, August 2008).

7 Standing Committee on Law and Justice, Parliament of NSW, *Remedies for the serious invasion of privacy in New South Wales* (Report No. 57, 3 March 2016).

8 *Grosse v Purvis* [2003] QDC 151; *Doe v Australian Broadcasting Corporation* [2007] VCC 281.

9 *Australian Broadcasting Corporation v Lenah Games Meats Pty Limited* (2001) 208 CLR 199, 258.

10 See for example *Richard v BBC* [2018] EWHC 1837 (Ch), *Mosley v News Group Newspapers* [2008] EWHC 1777 (QB), *His Royal Highness the Prince of Wales v Associated Newspapers Ltd* [2006] EWHC 11 (Ch), *Campbell v MGN Ltd* [2004] 2 AC 457, *Beckham v Mirror Group News Ltd* [2001] All ER (D) 307.

11 *Hosking v Runting* [2005] 1 NZLR 1 (CA).

12 *C v Holland* [2012] 3 NZLR 672.

While the legal position in the United States varies across state jurisdictions, there are numerous examples of claimants relying on some combination of state legislation and various amendments to the United States Constitution. These cases have resulted in very large awards of damages. Possibly the most significant privacy action was that commenced by former professional wrestler Hulk Hogan against Gawker Media, over the online publication of a sex tape, resulting in an award of $115 million in compensatory damages and $25 million in punitive damages, and the bankruptcy and eventual demise of Gawker Media.

While each of these jurisdictions has taken a different path, they have reached the same conclusion: that it is appropriate to offer a remedy to an individual who has suffered a serious invasion of privacy.

## The continuing need for reform

It is not clear why Australia has lacked an appetite for implementing reform in this area, although it may in part be due to what the ALRC observed in its 2014 report as a media that operates "more appropriately than some of their UK counterparts".[13] Instead, laws dealing with privacy in Australia are concerned with the circumstances in which individuals' personal information can be used, stored and disclosed by public and private bodies, as well as physical invasions of privacy (for example, common law torts of trespass and nuisance, and the equitable action for breach of confidence). There is some recognition on a state level,[14] but broadly speaking, Australian law has no remedy for the emotional distress suffered by an individual whose privacy is invaded.

Meanwhile, the damage that can result from an invasion of privacy remains significant. The types of harm identified by the ALRC in 1979,[15] including embarrassment by identification,[16] risk of physical danger by identification, and the distress of being photographed, recorded or filmed without consent,[17] remain as relevant as ever, if not more so in a digital age. The widespread availability of high resolution cameras and surveillance equipment and the ease with which images or information can be uploaded to the internet make it easier to disseminate private information,[18] while the transition of tabloid journalism to digital publication and a 24 hour news cycle have given rise to a constant demand for clickable content.

## What's next?

Looking forward, the inevitable next step will be another inquiry. In its response to the ACCC's Digital Platforms Inquiry Final Report, the Commonwealth Government announced its immediate intention to conduct a review of the *Privacy Act 1988* (Cth), considering "whether broader reform of the Australian privacy law framework is necessary in the medium- to long-term to empower consumers, protect their data and best serve the Australian economy", as well as considering the ACCC's recommendation to enable the erasure of personal information. In relation to the ACCC's recommendation to introduce a statutory cause of action of invasion of privacy, the Commonwealth Government's response was that such a reform would need to be considered as part of the aforementioned review.[19]

Despite the prospect of this issue once again being conflated with concerns about personal information and data, there is reason to remain hopeful that the separate issue of a cause of action for invasion of privacy will be embraced. Modern Australian society is increasingly aware of, and ascribes increasing value to, private spaces and private information. Political motivations that once made it unattractive to pursue reform are surely diminishing as public sentiment increasingly favours the protection of privacy.

The most likely model to be pursued going forward will be that endorsed by the Australian Law Reform Commission in its 2014 report, potentially with some minor modifications in recognition of subsequent developments in foreign jurisdictions. The cause of action would be established as a statutory tort under new Commonwealth legislation,[20] rather than through amendments to the *Privacy Act*, and so as to avoid the additional regulatory compliance burden that would be caused by approaching the issue at state level. The cause of action would have the following elements:

- The claimant's privacy was invaded, by way of either misuse of private information, or by 'inclusion upon seclusion' (for

13 Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Report No. 123, July 2014) [1.21].

14 *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 13; *Human Rights Act 2004* (ACT) s 12.

15 Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy* (Report No. 11, 1979), [228].

16 For example, the naming of victims of crime in news reports without their consent: *Doe v Australian Broadcasting Corporation* [2007] VCC 281.

17 For example, the rising phenomenon of revenge pornography, including in the context of a relationship breakdown as in *Giller v Procopets* [2008] VSCA 236.

18 Standing Committee on Law and Justice, Parliament of NSW, *Remedies for the serious invasion of privacy in New South Wales* (Report No. 57, 3 March 2016), 2.10 – 2.21.

19 Australian Government, *Regulating in the digital age: Government Response and Implementations Roadmap for the Digital Platforms Inquiry* (2019), 18.

20 Commonwealth power stems from the external affairs power, by means of Australia being a party to the International Covenant on Civil and Political Rights. Pursuant to Article 17, Australia has undertaken to adopt such legislative measures as may be necessary to give effect to the right of persons not to be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence.

example, a physical intrusion into the claimant's private space, or watching, listening to or recording private activities or affairs by electronic means).

- The claimant had a reasonable expectation of privacy, taking into account all relevant circumstances. This would include, at a minimum, the nature of the information, the means used to intrude or obtain the information, the place where the intrusion occurred, the purpose of the misuse or intrusion, the extent to which the information was already public, and the attributes and conduct of the claimant, including whether they "invited publicity or manifested a desire for privacy."
- The invasion of privacy was reckless or intentional. It is unlikely that a negligent invasion of privacy would suffice, although it is worth noting that the NSW Standing Committee on Law and Justice depart from the ALRC's model in relation to this issue.
- The invasion of privacy was sufficiently serious, having regard to factors including the degree of harm to an ordinary person in the claimant's position, and any malice.
- The claimant must satisfy the court that the public interest in privacy outweighs any countervailing public interest. This element, and the seriousness requirement, would ideally function to reduce any constraint on freedom of expression or freedom of the press, as well as taking into account factors like national security, public safety and the prevention and detection of crime.

There are some additional considerations that a future review may wish to take into account, including the available defences to a claim. A number of defences were recommended by the ALRC in 2014, including necessity, consent, fair report of proceedings of public concern, and publication of public documents.

There is the question of an appropriate limitation period, and whether, as was recommended by the ALRC in 2014 and is currently being considered by Defamation Working Party as part of its review of the Model Defamation Provisions, a single publication rule is appropriate, given the propensity for matters of this nature to involve online publications.

There is also a question of the type of claimant who may rely on such a cause: it has only been proposed to date that natural persons will have such a right, but it may be worth considering whether it is appropriate to extend this to a small class of excluded corporations, as is the case under the Model Defamation Provisions.

A future review would also necessitate analysis of recent developments in foreign jurisdictions, including the decision of the High Court of Justice in *Richard v BBC*,[21] which now restricts reporting of subjects of criminal investigations in the United Kingdom.

21 *Richard v BBC* [2018] EWHC 1837 (Ch).

# eSports - Is it a Sport, a Business or Both?

## A Look at the eSports Industry as it Enters a New Decade

**Emma Johnsen,** Senior Associate at Marque Lawyers, comments on previous decade of eSports and what's on the agenda for the 2020s.

Unless you've been hiding under a rock, or outside in fresh air engaging in outdoor sport, you will have seen the explosion of what is known as eSports (a.k.a. electronic sports). As the Washington Post recently noted: "In the years between 2010 and 2020, esports — organized, professional video game competition — grew from a niche, online subculture into a burgeoning cultural powerhouse. While such leagues and events had existed for years prior, it was this decade in which esports experienced major growth spurt."[1] Here, we provide a brief introduction into eSports and discuss what are the main issues facing the eSports industry in 2020 and beyond.

### What is eSports?

eSports is competitive video gaming. Whether eSports is considered a 'sport' is up for debate, however, what cannot be contested is that eSports has the ability to capture mainstream audiences globally and has grown into a billion dollar industry.

We are talking about global audiences of over 380 million, prize money of up to $25 million per tournament and crowds big enough to sell out Madison Square Garden three nights running. The eSports industry is tipped to have a market value of $1.79 billion US dollars by 2022 and global audiences expected to reach 557 million by 2021

### The minefield of legal issues

Think about a legal issue. Got one? It's probably an issue in eSports. The rapidly changing and complex industry triggers a range of commercial, policy and legal issues including broadcast rights, intellectual property, piracy, gambling regulation and employment issues. Doping and match fixing are also causing problems.

### Cheating in eSports

Just like any sporting competition, eSports has strict regulations to prevent cheating within the games. Referees in eSports tournaments monitor to ensure there is no rogue access to the internet or to the code, including by preventing the use of keyboards or mice which can allow for the new code to be installed.

With respect to ensuring integrity is upheld in the game in the industry, the Esports Integrity Coalition (ESIC) was established in 2015 to detail with "integrity challenges" to eSports which can include game hacking by way of software cheats, match fixing and online attacks which will cause opponents to slow down, or in some instances, entirely disable the opponent's game.

For example, in 2018, the ESIC placed a 5-year ban on player Nikhil "forsaken" Kumawat after he was caught cheating at a tournament in Shanghai. Tournament personnel had inspected Kumawat's computer and found that cheating software had been installed and upon inspection Kumawat tried to delete the software.

The ESIC works with a number of eSports companies and is charged with determining and issuing punishments as well as publishing Code of Conduct, an Anti-Corruption Code and an Anti-Doping Policy.

The ESIC has also recently announced the introduction of Talent Agent Regulations in January 2020 which is a global regulatory scheme introduced to talent agents. ESIC has stated that the overarching purpose of the scheme is to ensure youth protection and professional integrity in the administration of talent agent operations.[2]

### Lawsuits and investigations galore

With the rise in revenue streams and interest in the industry, comes the rise of lawsuits. One of the biggest lawsuits in the industry was filed by Turner 'Tfue' Tenney against eSports organisation FaZe Clan.

Tfue is one of the world's premier eSports players, with 120 million views on Twitch, more than 10 million YouTube subscribers and 5.6 million followers on Instagram. Initially filed in early 2019 in California (as that is where much of Tfue's work was undertaken) Tfue claims that Faze Clan's Gamer Agreement is unfair and predatory as it allegedly allows FaZe to take 80% of Tfue's revenue, and that the contract hinders Tfue from pursuing and earning money from sponsorship deals that FaZe Clan hasn't allowed.

FaZe Clan filed a counter-claim in August 2019 whereby FaZe alleged, among other things, misuse of confidential information and breach of contract. Relying on the

1 Will Partin, The 2010s were a banner decade for big money and tech - and esports reaped the rewards' *The Washington Post*, accessible at https://www.washingtonpost.com/video-games/esports/2020/01/28/2010s-were-banner-decade-big-money-tech-esports-reaped-rewards/.

2 https://esic.gg/esic-announces-introduction-of-talent-agent-regulations/

jurisdictional clause in the contract, the counter claim was filed in the federal district court in New York City and the matter has now morphed into a complex, multi-jurisdictional piece of litigation expected to be heard in March 2020.

Meanwhile back in Australia, the first major investigation into corruption in eSports commenced in 2019 after it was reported in September 2019[3] that Victoria Police were pursuing a number of eSports related criminal investigations following a number of reports being made to the Victoria Police force's Sporting Integrity Intelligence Unit about alleged match fixing in Counter-Strike: Global Offensive games. The investigations have raised concerns about what were described as 'clear shortcomings' in eSports governance, such as what publishers can do to assist in preventing corruption in the industry.

### What's the situation with IP in eSports?

eSports is a big web of licensed rights. Practically speaking, each different game could be thought of as a different "code" of eSport. The structure of rights in eSports is very top heavy, in that the individual publishers of each of the games have ultimate control over the rights to each game.

Under Australian copyright law, computer programs are protected by copyright. The game is also protectable as a cinematograph film. The owners of the rights in the games are typically the developers and publishers. The level of IP protection available to the owners of eSports is not available in 'traditional sport', meaning that the owners of each eSport have an increased level of control.

This creates an industry where the owners of each eSport can control the reproduction and dissemination of the game and, as a result, the ownership and exploitation of the IP rights is incredibly valuable. The owner of the eSport can then license the rights to the game to tournament organisers, broadcasters, merchandisers and sponsors.

One of the most precarious elements of the rise of eSports is with respect to 'Streamers' and the IP considerations that livestreaming brings. Streamers are not professional eSports players; they are personalities who run their own channels to which users can subscribe. Streamers can attract lucrative sponsorship contracts. However, the streamer may not have obtained the rights from the owner of the IP - in the particular eSport. This could cause downstream problems as streamers develop value in a brand which exploits a product in which they have no enforceable legal interest. Kind of a new form of cybersquatting. While it is the streamer who will usually retain any royalties generated from the views of their content, these streamers can actually help to assist the popularity of a game and as a result, the publishers will turn a blind eye to the copyright infringement that is taking place and in some instances actually assist the streamer to generate more views.

With eSports viewership tipped to make up 10% of all sports viewership in the US within the next 2 years, the industry is one to watch.



## 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**

3 https://www.abc.net.au/news/2019-09-24/fears-world-of-esports-is-ripe-for-corruption/11521008

# Telecommunications - A Decade of Change

**Joel von Thien,** Partner, and **Jonathan Selby,** Lawyer, at Clayton Utz, discuss the developments that took place in the telecommunications space in the 2010s and what is on the agenda for the coming decade.

The Australian telecommunications industry has transformed greatly over the last decade. This rapid change has been driven by technological advances, increased industry competition as well as new and upgraded network infrastructure. Australians have more choice than ever as the number of available telecommunications products and services continues to increase.

In response to this transformation, Australia's regulators have recognised the need to evolve the telecommunications regulatory framework to keep it fit for purpose.

In this article, we focus on how regulators have responded to a decade of industry change and review the regulatory developments in the key areas of consumer protections, access and interception of communications, telecommunications network security as well as spectrum management.

## Consumer protections

The appetite of consumers for internet and communications services surged throughout the last decade with Australians downloading almost 6 million terabytes of data in the 3 months to 30 June 2019 (enough to watch around 2.2 billion hours of HD video). This increase in demand has occurred alongside infrastructure investment in fixed line and mobile networks.

With the **nbn** network rollout nearing completion (approximately 7 million homes and businesses are connected to a plan over the **nbn** network and approximately 11 million homes and businesses are able to connect) and mobile communications becoming embedded in everyday life (over 85% of Australians own a smartphone), regulators recognised the need to reform Australia's consumer protection regime to deal with this new environment.

Key actions undertaken by regulators in this space have included:

## Consumer Safeguards Review

In 2018, the then Department of Communications and the Arts commenced the Consumer Safeguards Review to develop Australia's approach to telecommunications consumer safeguards for the future. The review, which is ongoing, has 3 parts:

- **Part A – redress and complaints handling**

  The Department published its report for Part A in 2018 and recommended a strengthened Telecommunications Industry Ombudsman scheme, changes to the ACMA's complaints handling standard and improved complaints reporting.

- **Part B – reliability of telecommunications services**

  The Department published its report for Part B in late 2019 and recommended:

  - wholesale level regulation of connections, repairs and appointment keeping timeframes to underpin whole of industry performance on connecting and repairing individual services;
  - retail level requirements for clear consumer information around any service commitments from retailers together with transparency of performance;
  - further consideration of well targeted and sustainable arrangements to maximise connectivity for medically vulnerable consumers; and
  - addressing existing reliability safeguards of limited and declining relevance.

- **Part C – choice and fairness in the retail relationship between the customer and their provider**

  This part is yet to commence.

## ACCC enforcement action and nbn Wholesale Service Standards Inquiry

Towards the end of the last decade, the ACCC stepped up its enforcement action against retail service providers for contravention of the Australian Consumer Law, particularly in relation to false and misleading advertising of services provided over the **nbn** network. In 2017, the ACCC published guidance for retail service providers on the advertisement of speeds in relation to broadband services, particularly the clear identification of typical peak speeds. The guidance was updated in 2019.

The ACCC also commenced the **nbn** Wholesale Service Standards Inquiry in 2017. In late 2019, the ACCC published its draft decision which indicated regulated terms are likely to be required to improve end user experiences on services provided over the **nbn** network. The ACCC is seeking to finalise the inquiry during the course of this year.

## ACMA initiated regulation

With a focus on dealing with consumer issues (and rising complaints) in relation to migration to the **nbn** network towards the end of the last decade, the ACMA introduced a number of new standards and other instruments designed to protect Australians in their dealings with retail service providers – these include:

- *Telecommunications (Consumer Complaints Handling) Industry Standard 2018*;
- *Telecommunications (Consumer Complaints) Record-Keeping Rules 2018*;
- *Telecommunications (NBN Consumer Information) Industry Standard 2018*;
- *Telecommunications (NBN Continuity of Service) Industry Standard 2018*; and
- *Telecommunications Service Provider (NBN Service Migration) Determination 2018*.

The ACMA has also been active in enforcing these new requirements by issuing fines and formal warnings to retail service providers for non-compliance.

## Communications Alliance initiated changes to Telecommunications Consumer Protections Code

The Telecommunications Consumer Protections Code, introduced in 2012, contains specific requirements for retail service providers around advertising, billing, changing retail service providers, complaints handling, customer contracts and sales practices.

Communications Alliance has consulted on and implemented a number of updates to the code throughout the last decade – the most recent in 2019, when the code was updated to introduce financial hardship provisions and align with the ACMA's consumer complaints handling standard.

## Access and interception of communications

Australia's regulatory framework in relation to the access and interception of communications has undergone a number of significant amendments over the last decade, reflecting the dynamic and evolving nature of the telecommunications industry as well as the challenges regulators must respond to.

The powers of law enforcement and security agencies to access and intercept information traveling over our telecommunications networks have progressively expanded over time with important implications for the industry.

Most recently, the assistance and access framework was significantly amended with the passage of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth). The amendments broadened the existing powers of law enforcement and security agencies to access communications and created new powers to compel assistance from a range of providers in the communications supply chain.

## Telecommunications network security

Recognising the increasingly significant role our telecommunications networks have come to play in Australia's economic and social wellbeing over the last decade, the Federal Government introduced the Telecommunications Sector Security Reforms in 2018.

The reforms introduced new obligations on:

- carriers, carriage service providers and carriage service intermediaries, to do their best to protect networks and facilities from unauthorised access and interference; and
- carriers and nominated carriage service providers, to notify government of planned changes to their systems and services that could compromise their capacity to comply with the security obligation.

The reforms also provided new powers to:

- the Secretary of the Department of Home Affairs, to obtain information and documents from carriers, carriage service providers and carriage service intermediaries, to monitor and investigate their compliance with the security obligation; and
- the Minister for Home Affairs, to direct a carrier, carriage service provider or carriage service intermediary to do, or not do, a specified thing that is reasonably necessary to protect networks and facilities from national security risks.

It is also notable that, in its 5G security guidance to Australian carriers, the Government effectively banned Chinese-based telecommunications equipment vendors from playing a role in the deployment of Australia's 5G networks. The Government advised carriers that *"the involvement of vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law, may risk failure by the carrier to adequately protect a 5G network from unauthorised access or interference"*.

## Spectrum management

There have been vast improvements in wireless technologies over the last decade. As a result, spectrum usage in Australia has changed significantly. Notably, Australians have become increasingly reliant on mobile networks to access the internet as Australia has moved from 3G (from 2006) to 4G (from 2011) to 5G (from 2019).

In response to these technological advances, the Federal Government has sought to reform spectrum laws. In late 2019, the Government committed to a staged approach to amend the *Radiocommunications Act 1992* (Cth). The amendments will be designed to remove unnecessary constraints in spectrum allocation and reallocation processes. A bill is expected to be introduced into Parliament this year.

Additionally, the ACMA has played an increasingly important role as Australia's spectrum manager. In 2018, the ACMA conducted a spectrum auction for the 3.6 GHz band which is a key band for 5G services. The 350 lots of 5 MHz each were sold to Dense Air Australia, Mobile JV, Optus Mobile and Telstra.

Earlier this year, in a major development for the deployment of 5G in Australia, the Federal Court approved a proposed merger between TPG and Vodafone on the basis it would not substantially lessen competition in Australia's retail mobile market. The merged entity of TPG and Vodafone may now deploy its own 5G network at more than 650 sites in Sydney, Melbourne, Brisbane, Adelaide, Perth, Canberra and the Gold Coast.

## Looking into the future

The completion and enhancement of the **nbn** network as well as the deployment of 5G mobile networks by Telstra, Optus and now TPG/Vodafone will continue the ever-accelerating demand for telecommunications products and services into the coming decade.

This new and upgraded infrastructure will also facilitate a range of emerging and innovative applications designed to provide economic and social benefits, improve the liveability of our cities and towns as well as enhance the way we access and interact with technology – these include:

- internet of things (IoT);
- smart cities;
- smart homes and businesses;
- e-heath;
- e-learning;
- enhanced law enforcement and security;
- entertainment applications; and
- autonomous vehicles.

Of course, these applications and others like them will create new challenges for regulators – particularly in the areas of consumer law, information and network security, privacy as well as health and safety. As always, legislators will need to strike a balance by implementing regulation that is necessary and proportionate while encouraging innovation and the use of our telecommunications infrastructure to its fullest capacity.

# 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)