Communications Law BULLETIN

CAMLA

Communications & Media Law Association Incorporated

Print Post Approved PP: 234093/00011

Talk Back - High Court Weighs in on 'Reply to Attack' Qualified Privilege

Sophie Dawson & Ben Teeger take a look at a recent decision by the High Court of Australia which considered the scope of the common law defence of 'reply to attack' qualified privilege in respect of defamatory statements made as a form of self-redress.

On 5 October 2012, the High Court of Australia delivered judgment in the defamation case of *Harbour Radio Pty Ltd v Trad*.[1]

The Facts[2]

In December 2005, a number of riots took place in various locations across Sydney. The riots involved a series of sectarian clashes between Australian Muslims and Australians of European descent. The riots became known as the 'Cronulla Riots' - Cronulla being the suburb in which the first of the riots took place.

On 18 December 2005, approximately one week after the Cronulla Riots, Mr Keysar Trad, a spokesman for the Muslim community in Australia, attended and delivered a speech at a rally in Hyde Park in Sydney. The rally was attended by approximately 5,000 people including representatives of the media. In his speech, Mr Trad attributed part of the blame for the Cronulla Riots to 2GB, which is a radio station owned by Harbour Radio Pty Limited (a subsidiary of Macquarie Radio Network Limited). Mr Trad accused 2GB and 'those racist rednecks in tabloid journalism' of being 'the mouthpiece of the Howard government', for mustering '5000 people filled with hatred' to participate in the Cronulla Riots and for causing suffering to the Muslim community in Australia more generally.

The following morning, Mr Jason Morrison, a presenter on 2GB, hosted, and 2GB broadcast, a segment which lasted for eleven minutes and which purported to respond to the comments made by Mr Trad the previous day (the ***Broadcast***). Mr Morrison described Mr Trad as a 'disgraceful individual' and a 'well-known apologist for the Islamic community spewing hatred and bile at anyone who did not agree with [his] philosophies and principles including this radio station'.

Procedural history

As the Broadcast was made before 1 January 2006, Mr Trad commenced a proceeding against 2GB in the Supreme Court of New South Wales under the *Defamation Act 1974* (NSW) rather than the *Defamation Act 2005* (NSW).[3] Mr Trad alleged that the Broadcast conveyed imputations which were defamatory of him. 2GB raised a number of defences, including substantial truth, contextual truth, fair comment and qualified privilege at common law.

---

1 Harbour Radio Pty Ltd v Trad (2012) 86 ALJR 1256.

2 The facts set out hereafter are a summary of the Court's findings: Harbour Radio Pty Ltd v Trad (2012) 86 ALJR 1256, 1260-1.

3 Harbour Radio Pty Ltd v Trad (2012) 86 ALJR 1256, 1259. The Defamation Act 2005 (NSW) only applies to publications made after 1 January 2006: see Defamation Act 2005 (NSW) sch 4 cl 2.

Volume 32 Nº 1
March 2013

Inside This Issue:

Contents

To be protected by the 'reply to attack' qualified privilege, journalists and media organisations should frame any reply to an attack such that it is commensurate with, relevant to and sufficiently connected with the attack

The jury found that eight of the imputations were conveyed in the Broadcast and were defamatory of Mr Trad. The imputations found to be defamatory were that Mr Trad:

(a) stirred up hatred against a 2GB reporter, which caused the reporter to have concerns about his own personal safety;

(b) incites people to commit acts of violence;

(c) incites people to have racist attitudes;

(d) is a dangerous individual;

(g) is a disgraceful individual;

(h) is widely perceived as a pest;

(j) deliberately gives out misinformation about the Islamic community; and

(k) attacks those people who once gave him a privileged position.

However, on 31 July 2009, Chief Judge at Common Law McClellan dismissed Mr Trad's claims with costs.[4] His Honour upheld 2GB's defence of qualified privilege for all imputations on the basis that the defamatory imputations conveyed during the Broadcast fell within the 'reply to attack' category of that defence. 'Reply to attack' privilege permits defamatory statements to be made as a form of self-redress.

Mr Trad appealed the primary judge's decision to the Court of Appeal of the Supreme Court of New South Wales on the applicability of the 'reply to attack' qualified privilege. On 22 March 2011, Justices Tobias, McColl and Basten unanimously reversed the decision of the primary judge in part.[5] Their Honours found that the defence of qualified privilege should not have applied to imputations (c), (h) and (k).

2GB applied for special leave to appeal part of the decision of the Court of Appeal to the High Court of Australia. 2GB sought to have the primary judge's initial finding on qualified privilege restored in respect of imputations (c), (h) and (k). Mr Trad sought to file a notice of cross-appeal, arguing that the defence of qualified privilege at common law was not available as the Broadcast was actuated by malice. Mr Trad also sought to have the defence of qualified privilege rejected for imputations (a), (b), (d), (g) and (j).

Decision

On 5 October 2012, a majority of the High Court of Australia:

- held that six of the eight defamatory imputations conveyed by 2GB (imputations (a), (b), (c), (d), (g) and (j)) were protected by the 'reply to attack' qualified privilege at common law, but that imputations (k) and (h) were not;
- remitted six of the defamatory imputations to the Court of Appeal for re-consideration of the substantial and contextual truth defences; and
- refused to grant Mr Trad leave to file a notice of cross-appeal.

Justice Heydon, in dissent, dismissed the appeal on the basis that 2GB had been actuated by malice as it had been reckless to the truth of imputation (a).[6]

4 Trad v Harbour Radio Pty Ltd [2009] NSWSC 750 (McLellan CJ at Common Law).

5 Trad v Harbour Radio Pty Ltd (2011) 279 ALR 183.

6 Harbour Radio Pty Ltd v Trad (2012) 86 ALJR 1256, 1271–5 (Heydon J).

plaintiffs should consider leading evidence which directly demonstrates that the defendant knew that their response was untrue (or were reckless as to its truth) at the time the reply to the initial attack was made

'Reply to attack' qualified privilege

Justices Gummow, Hayne and Bell (in a joint judgment), held that the 'reply to attack' qualified privilege at common law is available where a response to an attack is:

- commensurate with, relevant to and sufficiently connected with the attack; and
- bona fide for the purpose of vindication and not actuated by malice.

Their Honours found that a response may be 'sufficiently connected' with an attack by reference to the content of the attack, the credibility of the attack or the credibility of the attacker.[7] Justice Kiefel reached the same decision as their Honours but wrote a separate judgment. Her Honour found that the proportionality of the response only goes towards the issue of malice and not towards the issue of relevance.[8]

In addition, the response must be made in the discharge of a public or private duty or pursuant to an interest. In this case, the majority held that 2GB had an interest in publishing defamatory material to the general public in response to the public criticisms Mr Trad had made of it, and that the general public had an interest in receiving 2GB's response.[9]

The majority found that Mr Trad had not discharged his onus of proving that imputation (a) was actuated by malice, as he failed to lead evidence which directly demonstrated 2GB's state of mind at the time the Broadcast was made.[10] In the circumstances, it could not be said that 2GB knew that the facts which conveyed imputation (a) were untrue, or alternatively, were reckless as to its truth.

Substantial and contextual truth

The majority considered the test to be applied in considering whether material is defamatory and whether it is true. Their Honours preferred the approach of considering the truth defence by reference to 'an audience composed of ordinary decent persons, being reasonable people of ordinary intelligence, experience and education who brought to the question their general knowledge and experience of worldly affairs', which they considered to be the approach taken in *Radio 2UE Sydney Pty Ltd v Chesterton* (2009) 238 CLR 460.[11] The majority emphasised that the 'right thinking person' test traditionally applied seeks to eliminate extreme views and 'may be seen as a benchmark by which some views would be excluded from consideration as unacceptable', rather than requiring application of a moral or ethical standard.[12]

Given the partial success of both parties, the Court made no order as to the costs of the appeal and cross-appeal.

Implications

The decision suggests that:

- To be protected by the 'reply to attack' qualified privilege, journalists and media organisations should frame any reply to an attack such that it is commensurate with, relevant to and sufficiently connected with the attack. In considering any reply, thought should be given to whether the attack was public, and whether a public response will be commensurate with that attack. The reply must also be bona fide for the purpose of vindication and not actuated by malice.
- To defeat the defence of 'reply to attack' qualified privilege at common law on the ground of malice, plaintiffs should consider leading evidence which directly demonstrates that the defendant knew that their response was untrue (or were reckless as to its truth) at the time the reply to the initial attack was made.

Sophie Dawson is a partner and Ben Teeger a lawyer in the Technology, Media & Telecommunications team at Ashurst. The views expressed in this article are the views of the authors only and do not represent the views of any organisation.

---

7 Harbour Radio Pty Ltd v Trad (2012) 86 ALJR 1256, 1265–6 [33]–[35].

8 Ibid.

9 Harbour Radio Pty Ltd v Trad (2012) 86 ALJR 1256, 1263–4 [26], 1266 [36] (Gummow, Hayne and Bell JJ), 1282 [128]–[129] (Kiefel J).

10 Harbour Radio Pty Ltd v Trad (2012) 86 ALJR 1256, 1267 (Gummow, Hayne and Bell JJ), 1286 (Kiefel J).

11 Harbour Radio Pty Ltd v Trad (2012) 86 ALJR 1256, 1268 [54]–[56] (Gummow, Hayne and Bell JJ), 1287 [154] (Kiefel J).

12 Ibid.

Telecommunications Data Retention: A Step in the Right Direction?

Lisa Hill and Jessica Childs take a brief look at Australia's potential telecommunications data retention laws, which may form part of the Government's next package of reform of national security legislation.

Australian carriage service providers (***CSPs***) are currently not required to retain metadata associated with telecommunications services generally, for law enforcement or national security purposes. While it is usual for such data to be routinely retained by a CSP for business purposes (for example, billing, marketing and network monitoring purposes), associated storage costs mean that it will be deleted if no longer required. However certain metadata, such as the details of Uniform Resource Locators (***URL***) visited, is not likely to be retained for business purposes and therefore would be deleted immediately.

The Government has raised the possibility of introducing a European Union (***EU***) style telecommunications data retention regime with, "tai lored data retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities, and privacy and cost impacts"[1] (the ***data retention proposal***). Although the term "telecommunications data" is not defined in Australian legislation, the extrinsic materials suggest that it may mean the metadata associated with telecommunications services. Despite a lack of further detail on the Government's proposal – there is no draft legislation and no clear indication has been given as to the scope of the relevant data set - the issue has nevertheless ignited considerable debate on the merits and necessity of a data retention regime in Australia.

Inquiry by the Parliamentary Joint Committee on Intelligence and Security

In July 2012 the Government asked the Parliamentary Joint Committee on Intelligence and Security (***PJCIS***) to consider a package of potential reform of national security legislation. The Attorney General's Department released a discussion paper to accompany the relevant terms of reference and describe the reform proposals (the ***discussion paper***).[2] The discussion paper set out 18 proposals which were divided into 3 categories: those the Government wished to progress; those the Government is considering; and those on which the Government is seeking the views of the PJCIS.

The data retention proposal is included in the package of reform of the *Telecommunications (Interception and Access) Act 1979* (Cth) (the ***TIA Act***). At this stage the Government is only seeking the views of the PJCIS on the data retention proposal. Public submissions were sought by 20 August 2012. At the time of writing the PJCIS' report is yet to be tabled in Parliament.

Telecommunications data

Neither the discussion paper, nor any other documents available at the time of its release, provides adequate details and discussion of the nature of the data to be retained. As noted above, telecommunications data is not defined in either of the *Telecommunications Act 1997* (Cth) or the TIA Act, although the concept is relevant to these laws.

It is generally understood that telecommunications data refers to communications metadata; that is, information about a communication other than the content or substance of a communication, such as subscriber data (name and address) and traffic data (date, time, location and duration). However the scope of this information is not clear. In particular, it is not clear if, or to what extent, this information would include the URLs of websites visited by the customers of a CSP.

Statements made by the Attorney General, following the release of the discussion paper, have attempted to clarify the meaning of telecommunications data in the context of the data retention proposal. In a letter to the Chair of the PJCIS, the Attorney-General stated that the proposal does not include the retention of the content of a communication but rather the "*information about the process of a communication*" such as "*the identity of the sending and receiving parties and related subscriber details, account identifying information collected by the telecommunications carrier or internet service provider to establish the account, and information such as the time and date of the communications, its duration, location and type of communication*".[3] The Attorney-General has further clarified that this type of data does not include the content of phone calls, emails, "tweets" or posts,[4] nor does it include records of website visits.[5]

So, will the details of URLs visited be considered 'telecommunications data' for the purposes of the data retention proposal? The Government has previously reported that the general practice under the TIA Act has been that URLs will be telecommunications data "*to the extent that they do not identify the content of a communication*".[6] This approach is consistent with that proposed in the UK and under the EU data retention provisions. However, at the Senate Estimates hearings in October 2012, the Attorney-General's Department stated that in the context of the data retention proposal, data would not include records of web browsing and would not include URLs.[7] There is some merit in this approach given the large volume of data that could be generated from the retention of such information (being data which would not usually be retained by CSPs) and the fact that it may be otherwise accessible via generally available analytics tools.

Data retention periods

It is critical to understand why the Government is considering a two year data retention period, and whether this is likely to be effective in ensuring that law enforcement agencies have adequate opportunity to protect Australians against future telecoms and online communications threats, in view of privacy concerns and the heavy compliance cost burden on CSPs.

---

1 Attorney-General's Department, Equipping Australia Against Emerging and Evolving Threats, July 2012, p. 10.

2 Ibid.

3 Attorney-General's letter to Anthony Byrne MP, Chair of the PJCIS, undated, received by the PJCIS on 19 September 2012, p. 1.

4 N Roxon, Letter to the editor—Herald Sun, media release, 7 September 2012, viewed 7 January 2013, http://www.attorneygeneral.gov.au/Media-releases/Pages/2012/Third%20Quarter/7-September-2012-Letter-to-the-editor-Herald-Sun.aspxhttp://www.attorneygeneral.gov.au/Media-releases/Pages/2012/Third%20Quarter/7-September-2012-Letter-to-the-editor-Herald-Sun.aspx

5 R Epstein, Transcript of interview on ABC 774 Melbourne with Rafael Epstein and Joe Hockey, transcript, ABC Radio, 5 September 2012, viewed 7 January 2013, http://www.attorneygeneral.gov.au/Transcripts/Pages/2012/Third%20Quarter/5September2012-TranscriptofinterviewonABC774MelbournewithRafaelEpsteinandJoeHockey.aspx

6 Attorney General's Department, Telecommunications (Interception and Access) Act 1979 – Annual Report for the year ending 30 June 2011, p. 6.

The Attorney-General's Department's own advice on this issue was "*to limit the non-content data retention requirement to a short period (6 months) unless there is strong evidence relevant to Australia of the utility of a longer period*" before engaging in public consultation on a data retention proposal of up to two years. This recommendation is set out in a preliminary privacy impact assessment of the proposed reforms to the TIA Act that was conducted by Information Integrity Solutions and submitted to the department in December 2011.[8]

The Attorney-General's stated rationale for the data retention proposal (as part of a wider reform of national security legislation) is that the capabilities (systems, methods and tools) and powers of Australia's law enforcement and security agencies need to keep pace with cyber enabled crime and threats to national security.[9] Changing technology and business practices mean that less telecommunications data is now being retained by CSPs as a matter of usual business practice.[10] Accordingly, law enforcement and intelligence agencies claim that they cannot always access the data they need for investigations and that a longer retention period by CSPs would significantly increase their ability to operate in a digital environment as effectively as many criminals do now.[11]

Not surprisingly the data retention proposal has been met with significant resistance from CSPs. CSPs would ordinarily delete most communications data after they have completed their internal business processes, as such information is not currently required to be kept for law enforcement or national security purposes. Data storage costs and security concerns are their primary concerns. Similarly, consumer and user groups have also expressed privacy concerns, in relation to data security and privacy. For example, Electronic Frontiers Australia has expressed concerns about an "*unprecedented threat that [proposed data retention requirements] would represent to the right to privacy of all Australians*".[12] It is also not clear that any changes to the TIA Act in recent years have led to any great success measured in convictions per warrant issued.[13]

In relation to the length of the retention period, while the Government may have provided some rationale for data retention, to date there has been no discussion on whether a 2 year retention period would be appropriate for Australia. In relation to the issue of law enforcement's ability to access the data they need for investigations, there does not appear to be any publically available source in which, for example the Australian Federal Police, detail what proportion of their large number of requests for communications data were unsuccessful due to the data no longer being available from CSPs.[14] Understanding the scale of the issue for these agencies is difficult.

It would appear that the Government's justification for an Australian data retention regime relies heavily on the data retention directive for EU member states. The EU has had a data retention regime since 2006. Directive 2006/24 requires EU member states to oblige providers of publically available electronic communications services or of public communications networks to retain traffic and location data for between six months and two years, for the purpose of the investigation, detection and prosecution of serious crime.[15] However, it is questionable as to whether the EU regime has been successful in making the dent in serious or organised crime that the EU had intended.

In a 2011 review of Directive 2006/24 by the European Commission, the '*Evaluation report on the Data Retention Directive*' reported that quantitative evidence provided by EU member states regarding the age of retained data showed that around ninety percent of the data is six months old or less and around seventy percent three months old or less, when the initial request for access is made by law enforcement authorities.[16] Most of the EU member states who had transposed Directive 2006/24 into local law had opted for retention periods of less than 2 years (mainly 6 months to 1 year).[17] The report also found that the Romanian Constitutional Court in October 2009, the German Federal Constitutional Court in March 2010 and the Czech Constitutional Court in March 2011 annulled the laws transposing Directive 2006/24 into their respective jurisdictions, on the basis that they were unconstitutional.[18]

Despite a lack of further detail on the Government's proposal the issue has nevertheless ignited considerable debate on the merits and necessity of a data retention regime in Australia

The EU data retention experience raises serious questions as to whether Australia should be using principles from this EU regime, as an example of an effective method of data retention. The Government needs to analyse the effectiveness of both the EU regime and the proposed Australian regime, if the changes proposed are to be consistent with evidence-based policy approaches.

Next steps

With a federal election date of 14 September 2013 now locked in, there is no certainty that the PJCIS' report, including the Committee's views on the data retention proposal, will be tabled in Parliament this year. Given the Government's recent release of a new national security strategy package, it is also doubtful that any draft national security reform legislation could be published before the election. Therefore, national security reform legislation, with data retention provisions, is not likely to pass through the current Parliament.

With the Coalition unlikely to oppose the data retention proposal in principle, if such legislation enacted in a future Parliament then it would be more efficient for CSPs to pass on any associated costs of implementing the regime to the customer, rather than have the Government foot the bill. As a result, CSPs will need to consider how to manage their customer relationships when passing on such costs.

Lisa Hill is Special Counsel at Webb Henderson. Jessica Childs is Corporate Counsel at Optus. The authors would like to thank Dr Rob Nicholls of Webb Henderson for his assistance with this paper.

The views expressed in this article are the views of the authors only and do not represent the views of any organisation.

---

7 Senate Hansard, Legal and Constitutional Affairs Legislation committee, Estimates, 16 October 2012, p. 90

8 Information Integrity Solutions, Privacy Impact Assessment - Preliminary Report – Telecommunications (Interception and Access) Act 1979 Reform, December 2011, p. 12. Released publicly for the first time in August 2012 under freedom of information laws.

9 Attorney-General's Department, Equipping Australia Against Emerging and Evolving Threats, July 2012, p. 3.

10 Attorney-General's letter to Anthony Byrne MP, Chair of the PJCIS, undated, received by the PJCIS on 19 September 2012, p. 2.

11 See for example, the Australian Federal Police submission to the PJCIS *Inquiry into potential reforms of National Security Legislation*, submission no. 163, p.15-18.

12 Electronic Frontiers Australia Inc, submission to the ,PJCIS' *Inquiry into potential reforms of National Security Legislation*, submission no. 121, 2012, p.5.

13 Nicholls, Rob "Right to Privacy: Telephone Interception and Access in Australia", Technology and Society, 31 4 Spring 2012.

14 Ibid at p. 14.

15 Available at ://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

16 European Commission, Report from the Commission to the Council and the European Parliament – Evaluation report on the Data Retention Directive, 18 April 2011, p. 15, https://www.eff.org/sites/default/files/filenode/dataretention/20110418_data_retention_evaluation_en.pdf

17 Ibid at p. 14.

18 Ibid at p. 5.

The Courts v Twitter: The Future of Live Court Reporting in NSW

Chris Paver examines the use of Twitter in courtrooms and the challenges posed by social media to the administration of justice.*

NSW Attorney General Greg Smith's attempt to tighten a loophole in court security laws has drawn attention to an emerging battleground for today's Internet-savvy court reporters. In a Bill[1] introduced in late 2012, he proposes to ban the use of devices like smartphones or laptops to transmit sounds, images or information "that forms part of the proceedings of a court" from inside courtrooms or places where courts are sitting. All of a sudden, it appeared that journalists caught Tweeting, blogging, texting and even emailing from court could face fines of up to $22,000 and a year in jail – a hefty penalty for simply reporting on the activities of the court.[2] Following concerns discussed in the press, Smith has now clarified that journalists and lawyers will be exempt from the restrictions under a new regulation[3] – essentially leaving the question of live tweeting to the courts.

How, for example, can the courts ensure the due administration of justice when any member of the public, armed only with a mobile phone, could easily transmit live what one witness says in court to another witness waiting outside to give evidence?

Explaining the amendments in Parliament, Smith said they were intended to address "recent security incidents" that highlighted the law's failure to keep pace with modern technology.[4] How, for example, can the courts ensure the due administration of justice when any member of the public, armed only with a mobile phone, could easily transmit live what one witness says in court to another witness waiting outside to give evidence? While the planned media exemption may soften the blow for journalists, however, it also illustrates the need for legislators and the courts to redefine the fundamental principle of open justice in the digital age.

A step in the wrong direction

In late 2011, the Lord Chief Justice of England and Wales, Lord Judge, delivered new guidance allowing journalists to Tweet from inside courtrooms, without seeking permission. He was aware of the risks, especially in the context of criminal trials, but concluded:

> "A fundamental aspect of the proper administration of justice is open justice. Fair, accurate and, where possible, immediate reporting of court proceedings forms part of that principle."[5]

Under the guidance, judges retained the right to prohibit live, text-based reporting in the interests of justice. Less than two months later, the judge in a high profile case did just that after a Twittering journalist was believed to have used the service both to name a juror and report on matters discussed in the absence of the jury, according to media reports.[6] The case, and several others internationally, highlight the well-documented risks that instant publication can pose in the context of the courts.

Such examples raise concerns, but as social media continues to play a greater role in our daily lives, how far should NSW courts go to restrict its use? More importantly, could an overly aggressive approach restrict scrutiny and cement impressions that the courts are out of touch? It has been noted on numerous occasions that greater transparency and public access can boost public understanding of and confidence in the judicial process.[7] In the High Court of Australia, it has been observed that 'the public administration of justice tends to maintain confidence in the integrity and independence of the courts.'[8]

Introducing the Bill last year, Smith emphasised that the motivation behind the proposed ban was not to target journalists. He said:

> "…it is important to preserve the principle of open justice. Although not common, there may be circumstances in which journalists wish to use electronic devices to report on proceedings contemporaneously through new media, such as Twitter or by blogging."[9]

He went further in February, stating that:

> "Under the exemption, journalists will have the same freedom to report on court proceedings as they do under the current

1 Courts and Other Legislation Further Amendment Bill 2012 (NSW), Schedule 1 Item 1.8.

2 Ibid.

3 James Hutchinson and Alex Boxsell, NSW waters down court social media laws (19 February 2013), The Australian Financial Review, < http://www.afr.com/p/technology/nsw_waters_down_court_social_media_X6dcNSKJThJ5nMX0w7C7gM>

4 New South Wales, Parliamentary Debates, Legislative Assembly, 21 December 2012 (Greg Smith, Attorney General).

5 Judiciary of England and Wales, Guidance on Live, Text-Based Communications from Court (14 December 2011) <http://www.judiciary.gov.uk/publications-and-reports/guidance/2011/courtreporting>.

6 Andrew Pugh, Twitter ban at Redknapp trial after reporter names juror (25 January 2012) Press Gazette <http://www.pressgazette.co.uk/node/48623>.

7 Adriana C. Cervantes, 'Will Twitter Be Following You in the Courtroom?: Why Reporters Should Be Allowed to Broadcast During Courtroom Proceedings' (2011) 33:1 Hastings Communications and Entertainment Law Journal 150. See also Chief Justice of Canada Beverley McLachlin, 'The Relationship between the Courts and the News Media' in Patrick Keyzer, Jane Johnston and Mark Pearson, The Courts and the Media (Halstead Press, 2012) 24, 26.

8 Russell v Russell [1976] HCA 23, 8 (Gibbs J).

9 Hansard, above n 4.

court policies. They will continue to be able to use their phone or other electronic device to transmit information to colleagues outside the court, unless ordered otherwise by the judge."[10]

The statutory changes themselves do not provide an exemption for journalists. However, they emulate other provisions allowing judges to grant exemptions,[11] which means journalists could continue to tweet as long as the judge approved. The NSW Government has also consulted with media organisations to draft the regulations that will create an exemption for journalists. More complex questions about the status of citizen journalists and bloggers, however, remain unanswered. The question also arises, why not simply include the exemptions in the amendments? Media lawyer Kevin Lynch argues that without clear statutory exemptions, regulations could be changed without being reviewed by the Parliament. "If you're going to put a restriction which has the potential of restricting freedom of speech it's best that you're quite clear about the limits of those restrictions when you actually write the law," he said.[12]

The NSW Government's amendments come at a time when many courts themselves are becoming more proactive about improving public access. The Supreme Court of Victoria, for example, already has its own Twitter account with more than 1,300 followers, webcasts some of its key decisions online, and is reviewing its policy in relation to court reporting via Twitter.[13] On the other hand, Victoria has also been singled out for criticism in recent years over the excessive use of suppression orders.[14] In Queensland courts, reporters can already use laptops to live-Tweet proceedings, while in South Australia, a working party is now considering the use in court of live text-based forms of communication, including Twitter, with a view to producing a Practice Direction for the Supreme and District Courts.[15] In each of these examples the courts have recognised that digital and social media have forever changed the way in which people access information and communicate with each other. As Keyzer notes, the notion that we are still willing to wait until the evening news for information about what is happening in the courts seems "not just antiquated but bizarre".[16]

In this context, Smith's earlier assertion that circumstances where journalists wish to report live via Twitter are "not common" is also unlikely to stand the test of time. There is little wonder that many journalists and media organisations more broadly have already embraced Twitter and other powerful new tools like Facebook to instantly report to thousands of people, satisfying our itch for immediate access to information. Indeed, some media reports suggest journalists are already routinely tweeting and texting from court, perhaps even without the knowledge of judges and magistrates.[17]

Twitter and the Courts

Journalists using Twitter to report on court proceedings is by no means a new phenomenon. In Australia, the R*oadshow Films Pty Ltd v iiNet Limited* copyright case in the Federal Court is widely acknowledged as the first case to be live-tweeted. In that case, Justice Cowdroy opted not to stop two journalists from using Twitter, noting in his judgment that he granted approval "in view of the public interest in the proceeding, and it seems rather fitting for a copyright trial involving the Internet".[18] Interestingly, in the end The Australian's publisher News Limited pulled the plug on journalist Andrew Colley's tweets, a spokeswoman highlighting that content should be published on "company properties" and that the company faced a risk when it could not "legal" journalists' content.[19]

The wariness some judges and legislators have shown about the capacity for social media to be used either deliberately or inadvertently to derail judicial process is understandable

Other courts have taken a different approach. In 2011, a Victorian magistrate chose to put a stop to tweeting during committal proceedings against a former police officer accused of leaking information to The Australian about a planned anti-terror raid.[20] Magistrate Peter Mealy warned journalists that tweeting the case would amount to contempt of court, explaining that it was inappropriate because statements made could later be suppressed or be the subject of objection.

The debate now taking place in NSW again highlights the challenges that social media poses to the courts as they search for the right balance between open justice in the digital age on the one hand, and the due administration of justice on the other. As Keyzer observes, "digital and social media have tipped the balance decisively in favour of freedom of communication".[21]

The wariness some judges and legislators have shown about the capacity for social media to be used either deliberately or inadvertently to derail judicial process is understandable. The "central thesis" of the administration of criminal justice, after all, is the entitlement of the accused to a fair trial under the law.[22] A simple Google search instantly reveals dozens of examples of where the Internet,

10 New South Wales, Parliamentary Debates, Legislative Assembly, 19 February 2013 (Greg Smith, Attorney General).

11 *Court Security Act 2005* (NSW) s 9(2)(a).

12 Stephanie Quine, Technology ban may not be smart move (17 January 2013), Lawyers Weekly, < http://www.lawyersweekly.com.au/news/technology-ban-may-not-be-smart-move >.

13 Email correspondence from Michelle Dall to Christopher Paver, 21 January 2013.

14 John Hartigan, 'The Courts and the Media in the Digital Era: A Media Perspective' in Patrick Keyzer, Jane Johnston, Mark Pearson The Courts and the Media (Halstead Press, 2012) 16, 18 and 22.

15 Email correspondence from Sylvia Kriven to Christopher Paver, 18 January 2013.

16 Patrick Keyzer, 'Who Should Speak for the Courts and How? The Courts and the Media Today' in Patrick Keyzer, Jane Johnston, Mark Pearson The Courts and the Media (Halstead Press, 2012) 5-6.

17 Nic Christensen, Reporters' live tweeting from court risks mistrials (5 December 2011) The Australian <http://www.theaustralian.com.au/media/digital/reporters-live-tweeting-from- court-risks-mistrials/story-fna03wxu-1226213631453>.

18 *Roadshow Films Pty Ltd v iiNet Limited (No. 3)* [2010] FCA 24.

19 Sally Jackson, Judges have final decision after Twitter enters court (19 October 2009) <http://www.theaustralian.com.au/media/judges-have-final-decision-after-twitter-enters-court/story-e6frg996-1225788100101>.

20 Chip Le Grand and Pia Akerman, With court a'Twitter, magistrate bans tweets (4 November 2011) The Australian <http://www.theaustralian.com.au/media/with-court-atwitter-magistrate-bans-tweets/story-e6frg996-1226185137003>

21 Keyzer, above n 16.

22 *McKinney v The Queen* (1991) 171 CLR 468, 478.

and social media in particular, have clashed with courtroom rules and traditions and, in some instances, prejudiced a case. In the United States, a Kansas judge declared a mistrial in a murder case after a reporter tweeted a grainy photograph from inside the courtroom featuring the profile of a juror.[23] Jurors themselves have even ventured online, one famously taking to Facebook to declare it was "gonna be fun to tell the defendant they're GUILTY". The person in question was dismissed from the jury and slapped with a fine and a five--page essay on the right to a fair trial.[24]

courts are now, more than ever before, able to use technology to communicate directly with the public rather than relying exclusively on the mainstream media

Associate Professor of Journalism and Public Relations at Bond University, Jane Johnston, identifies four primary issues upon which concerns about tweeting from court are based:

- interruptions to proceedings;
- the fact that tweets are limited to 140 characters and cannot reflect context;
- the temptation to use smartphone cameras; and
- the capacity for people without knowledge of the laws of contempt or defamation to tweet from court.[25]

She notes that the first three arguments also applied to the well--documented issue of whether television cameras should be allowed in court, which, despite recent progress,[26] remains a sore point for the mainstream media.[27]

In relation to the idea that tweeting journalists might disrupt proceedings, the nature of the process itself suggests the contrary. In fact, it seems more likely that a journalist typing quietly on a laptop would cause no more distractions to the court than one scribbling on a notepad, and far fewer than one constantly leaving so they can tweet outside.[28]

It is obvious that a 140 character Tweet will never achieve the level of detail of a full court report or broadcast. For those who believe the media already focuses too much on sensational details and fails to report comprehensively, the shorter word count is hardly likely to inspire confidence. Of course in the case of Twitter, journalists are able to create hashtags in order to make their tweets easily searchable, arguably creating a more complete report.[29] However, there is no guarantee that individual tweets would not be read in isolation or be re-tweeted by to a wider audience. South Australia's Victims of Crime Commissioner Michael O'Connell has also warned that Tweeting carries with it the risk of "making a case sound more sinister", emphasising the need for stronger laws to protect the privacy and rights of victims.[30]

On the other hand, the Supreme Court of Victoria's decision to take to Twitter to report its own decisions clearly reflects its belief that 140 characters is enough to accurately reflect the outcome of a case. In the United Kingdom, Lord Judge's practice guidance on live, text base reporting presumes that journalists tweeting during court cases are using their devices for the purpose of producing fair and accurate reports.[31] Trained journalists also typically have a strong understanding of legal restrictions that already exist on court reporting, whether in print, broadcast or online. Of course, not all court reporters – or, indeed, citizen journalists or members of the public - may choose to use Twitter inside courtrooms. However, the fact that that they could simply leave the room and tweet from outside without breaching the law also brings into question the utility of the proposed restrictions.

The Supreme Court of Victoria's decision to use Twitter highlights another important aspect of the social media debate: that the courts are now, more than ever before, able to use technology to communicate directly with the public rather than relying exclusively on the mainstream media. The media remains vital. However, Victorian Chief Justice Marilyn Warren has noted:

> "The courts are getting to a stage where they have had enough of the inappropriate criticism, the skewing of information in the media, and we really need to try and seize the day ourselves and give some information to the community."[32]

Clearly, it is possible that social media could be used more widely to enhance the amount of information available to both journalists and members of the public.

A similar argument could be made in relation to the regulation of court reporting and attempts by the courts to suppress information that could taint witnesses or jurors or impinge on the rights of people involved in a matter. As Stepniak observes:

> "The internet is clearly not restricted by geographical boundaries of jurisdictions and by expectations that memory will fade with the passing of time – core factors on which contempt laws are premised. In the light of such implications of new technology courts may well need to protect the administration of justice through dissemination of accurate information rather than through increasingly ill-suited attempts at suppression."[33]

---

23 Beth Stebner, Reporter causes mistrial in murder case by tweeting photos of juror – after judge warned against it (12 April 2012), Mail Online < http://www.dailymail.co.uk/news/article-2128556/Reporter-causes-MISTRIAL-murder-case-tweeting-photo-including-grainy-profile-juror--judge-warned-it.html>; AP, Reporter's photo causes mistrial in Austin Tabor drug murder case (11 April 2012) Huffington Post < http://www.huffingtonpost.com/2012/04/11/reporter-photo-austin-tabor-case-mistrial-declared-ann-marie-bush_n_1418723.html>

24 Ed White, *Judge punishes Michigan juror for Facebook post* (2 September 2010) The Seattle Times, <http://seattletimes.com/html/nationworld/2012785464_apusfacebookjuror.html>.

25 Jane Johnston, 'Courts' New Visibility 2.0' in Patrick Keyzer, Jane Johnston, Mark Pearson, The Courts and the Media (Halstead Press, 2012) 41, 45.

26 See Daniel Stepniak, 'Cameras in Court: Reluctant Admission to Proactive Collaboration' in Patrick Keyzer, Jane Johnston, Mark Pearson The Courts and the Media (Halstead Press, 2012) 66.

27 Hartigan, above n 14, in Keyzer et al, 21.

28 Mark L. Tamburri, Thomas M. Pohl, and M. Patrick Yingling, 'Twitter in the Courtroom' (2010) 15 Electronic Commerce & Law Report 1415; Adriana C. Cervantes, 'Will Twitter Be Following You in the Courtroom?: Why Reporters Should Be Allowed to Broadcast During Courtroom Proceedings' (2011) 33:1 Hastings Communications and Entertainment Law Journal 152.

29 Jacqui Ewart, 'Terrorism, the Media and Twitter' in Patrick Keyzer, Jane Johnston, Mark Pearson *The Courts and the Media* (Halstead Press, 2012) 55, 65.

30 Sean Fewster, South Australian lawyers say live tweeting from the court room is OK (17 July 2012) Adelaide Now <http://www.adelaidenow.com.au/news/south-australia/south-australian-lawyers-say-live-tweeting-from-the-court-room-is-ok/story-e6frea83-12264285261877>.

31 Judiciary of England and Wales, above n 5.

32 AAP, Victorian courts look at tweeting rulings (1 September 2011) CIO <http://www.cio.com.au/article/399317/victorian_courts_look_tweeting_rulings/>.

33 Stepniak, above n 33, 77.

In NSW, the proposed restrictions focus on instantaneous communication – attempting to stop people with "malicious intentions" from disrupting the work of the courts.[34] However, the challenges social medial poses to the criminal justice system are broader. Johnston refers to several examples of high profile criminal cases where discussions on Facebook and blogs have "raised significant problems for the administration of justice",[35] such as the seven and a half year search for Sunshine Coast teenager Daniel Morcombe which resulted in a 42-year-old man being charged. More recently, social media users have been urged to exercise restraint and caution in their comments online about the death of Jill Meagher, in case they prejudice the trial of the man charged with her murder.[36] One Facebook hate page had reportedly attracted about 44,000 'Likes'.[37] The Herald Sun reported that Victoria would push for national laws to reduce the risk that comments on social media sites like Facebook could influence juries and thus compromise criminal trials.[38]

As Burd and Horan note, such prejudicial publicity is only a click away for the "Googling juror".[39] While the courts have numerous mechanisms to help prevent prejudicial publicity affecting jury trials – such as suppression orders and contempt laws, and jury directions to prevent juror misconduct like conducting Internet searches – several commentators believe these remedies have become less effective in the digital age. Some even propose trials by judge alone in certain cases.[40] In relation to the live communication covered by the planned amendments in NSW, the Chief Justice of Canada, the Right Honourable Beverley McLachlin's observation is pertinent: "If witness or juror contamination is a concern with television, is it not even more so with ubiquitous social media accessed or received automatically via a hand-held device?"[41] This issue is yet to be satisfactorily addressed.

Conclusion

In the digital age, the principle of open justice – and its corollary that is the right of the media to report on court proceedings[42] – must go further than simply granting access to the courtroom. It is arguable that instant reporting, including journalists' use of Twitter to report on the activities of the court, is important to "increase transparency and public understanding of the judicial process".[43] Serious consideration should therefore be given to the merits of allowing live court reporting where appropriate. In NSW, the state government's proposal to modernise outdated court security laws seeks to address another important issue: ensuring that modern technology is not used to compromise the administration of justice. Without carefully crafted exemptions for journalists as a minimum, however, the threat to open justice is clear. As such, until the effect of the exemption for the media is known, exactly where that balance will lie in NSW remains uncertain.

Chris Paver is a law graduate and a former journalist who is currently completing his practical legal training at the University of Technology, Sydney.

*This article is based on Chris' winning entry into the 2012-2013 CAMLA Essay Competition.

---

34 Smith, above n 10.

35 Johnston, above n 32, 46.

36 Adrian Lowe, 'Trial by social media' worry in Meagher case (28 September 2012) The Age <http://www.theage.com.au/technology/technology-news/trial-by-social-media-worry-in-meagher-case-20120928-26pe4.html>.

37 Marianna Papadakis, Social media threatens justice in Jill Meagher murder case (1 October 2012)

<http://www.afr.com/p/national/social_media_threatens_justice_in_GXfIGAuxkDLEB2LzThiHTN>.

38 Grant McArthur, Victoria to push for new national laws to cut the risk that social media will jeopardise trials (2 October 2012), <http://www.heraldsun.com.au/news/victoria/victoria-to-push-for-new-national-laws--to-cut-the-risk-that-social-media-will-jeopardise-trials/story-e6frf7kx-1226486126154>.

39 Roxanne Burd and Jacqueline Horan, 'Protecting the right to a fair trial in the 21st century – has trial by jury been caught in the world wide web?' (2012) 36 Criminal Law Journal 103, 106.

40 Elizabeth Greene and Jodie O'Leary, 'Ensuring a Fair Trail for an Accused in a Digital Era: Lessons for Australia' in Patrick Keyzer, Jane Johnston, Mark Pearson The Courts and the Media (Halstead Press, 2012) 101, 119.

41 Chief Justice of Canada Beverley McLachlin, 'The Relationship between the Courts and the News Media' in Patrick Keyzer, Jane Johnston, Mark Pearson The Courts and the Media (Halstead Press, 2012) 24, 33.

42 *John Fairfax Publications Pty Ltd v District Court of NSW & Ors* [2004] NSWCA 324, 20 per Spigelman CJ.

43 Cervantes, above n 7, 158

Striking a Balance: News Regulation in the Digital Age

Jarrod Bayliss-McCulloch sets out an approach to news regulation that balances a variety of competing interests.*

News and media commentary play a vital role in a democratic society, and no regulation should endanger that role.[1] However a free press also wields great power; power to influence political processes that go to the heart of a democracy, and power to cause harm both to individuals and organisations, if unchecked. As a result, a level of regulation is necessary to ensure that media news and commentary meets appropriate journalistic standards in fairness, accuracy and transparency, and that news publishers are publicly accountable for the content they produce. This paper considers the need for cross-platform ethical standards in the "converged" news media environment of the digital age and sets out a preferred approach to news content regulation that seeks an appropriate balance between the legitimate commercial interests of big media and the public interest in access to quality, accurate and transparent news journalism.

Media organisations have been outspoken about the challenges involved with adapting to this new media environment, and any increased regulation that may come with it, as they try to develop new revenue streams to fund the ongoing production of quality content

The challenges of news regulation in the digital age

Striking an appropriate regulatory balance for news content is more of a challenge in today's digital age than ever before, as digitisation of news content is "blurring the traditional distinctions between broadcasting and other media across all elements of the supply chain, for content generation, aggregation, distribution and audiences",[2] creating a new and radically different media ecosystem[3] to which our regulatory frameworks must adapt. The transformations are not only about the way traditional media operates and is delivered. They also relate to consumer behaviour and interaction, as traditional one-to-many forms of news communications such as print, radio and television, with predictable forms of content delivery and platforms, give way to user-generated content and social media, empowering individuals to take on media-like roles in the online environment.

There are new and different voices with varying degrees of professionalism and commercialism: online opinion papers, blogs, citizen journalists and social media sites are all contributing to the discourse.[4] Media organisations have been outspoken about the challenges involved with adapting to this new media environment, and any increased regulation that may come with it, as they try to develop new revenue streams to fund the ongoing production of quality content.[5] Certainly there is a need for sensitivity in this context, understanding that a regulatory burden that is too onerous may discourage investment and create financial difficulties for Australian media organisations navigating the complex waters of new media technologies and revenue models. The challenges however are equally great for regulators who have a weighty responsibility to ensure that quality content is produced and made available across platforms, even as the nature of the relationship between content provider and delivery platform and audience and producer changes.

In this context, traditional vertical, silo-based approaches to regulation can no longer be justified.[6] International jurisdictions such as Malaysia, the European Union, the United Kingdom, South Africa, Korea, Japan and Taiwan have already recognised this, moving toward converged legislative frameworks that favour a platform-neutral approach,[7] and now Australia seems ready to follow suit. In this broader context, the Convergence Review (***Review***) recently advocated a "technology-neutral approach [to news content regulation] that can adapt to new services, platforms and technologies,"[8] and similarly, the core recommendation of the recent Independent Inquiry into the Media and Media Regulation (***Inquiry***) is to establish a single platform-neutral regulatory body overseeing all news producing media.[9] The notion of cross-platform consistency represents a welcome shift in thinking in a media environment where the same content can now be simultaneously delivered across a range of platforms. There remain, however, significant questions

1 The Hon R Finkelstein QC, *Report of the Independent Inquiry into the Media and Media Regulation,* February 2012, www.dbcde.gov.au/digital_economy/independent_media_inquiry, at 7.

2 Australian Communications and Media Authority [hereinafter ACMA], Digital Australians—Expectations About Media Content in a Converging Media Environment: Qualitative and Quantitative Research Report (2011), 7.

3 See Hitchens, L "Media Regulatory Frameworks in the Age of Broadband: Securing Diversity" Journal of Information Policy 1 (2011): 217-240.

4 Ibid, 222.

5 See, for example, News Ltd CEO Kim Williams' Speech to Melbourne Press Club, November 28, 2012, transcript online at http://www.theaustralian.com.au/news/a-bright-future-for-australian-journalism/story-e6frg6n6-1226525782027, accessed 11 January 2013.

6 Hitchens, above n 3, at 220.

7 ACMA, Converged legislative frameworks - International Approaches, Occasional Paper, July 2011, available at http://engage.acma.gov.au/convergence-international-approaches/.

8 Australian Government, Convergence Review, Final Report, March 2012, xvi.

9 Finkelstein, above n 1.

10 Weaknesses in the current regulatory framework were discussed extensively in the Inquiry: Ibid, 8.

around what that platform-neutral approach should look like when it comes to the regulation of news media content.

There are compelling reasons why a revised regulatory structure is needed to achieve the degree of responsible journalism desirable in a democracy in the digital age, which are apparent by reference to the inadequacies of the current regulatory framework.[10]

All news media are subject to basic external regulation including the laws of defamation and contempt. Beyond that, regulation currently differs by platform, with broadcasters subject to statutory regulation overseen by the Australian Communications and Media Authority (***ACMA***), while newspapers are subject to less onerous mechanisms of self-regulation, and online news is not extensively regulated at all. Of the existing self-regulation measures, only one or two newspapers have appointed an ombudsman or reader's representative and online news publications are not covered. The Australian Press Council (***APC***), which currently handles complaints from the public and monitors professional standards, is regularly criticised on the basis that it lacks the necessary funds and powers to carry out its functions effectively, and is subject to the voluntary support of the publishers it is intended to regulate; if a media organisation becomes dissatisfied with the APC it can simply leave and set up its own complaints handling body.[11] Problems with the regulation of news media were recognised by the Senate Select Committee on Information Technologies in 2000,[12] when it found deficient 'the efficiency and effectiveness of self-regulation…' and stated that '[s]elf-regulation in the print media industry appears to be failing the community.' These partially ineffective self-regulatory measures may be contributing to the low levels of trust and public confidence in the media identified in the course of the Inquiry.

Media outlets place great faith in the law of defamation as a check on journalistic practices.[13] However, legal proceedings against the media in cases of serious wrongdoing are protracted, expensive and adversarial, and offer redress only for narrowly defined legal wrongs, rather than complaints about accuracy or unfairness. The Inquiry cited a recent example of Mark French, a professional cyclist, who sued the publisher of the Herald Sun over an article published six years earlier that suggested Mr French was a drug cheat.[14] Following a trial lasting six days, Mr French was awarded $175 000 in damages and the publishers were ordered to pay his legal costs. In the course of that trial, Mr French paid $893 000 in costs. Even if he recovers two-thirds of those costs, Mr French, a successful litigant, will be out-of-pocket by more than $100 000.

The challenges presented by a convergent media landscape provide an opportunity to reconsider current regulatory measures in favour of more practical, efficient and effective cross-platform measures that provide positive outcomes for those who suffer harm due to poor media conduct, and promote responsible journalistic practices to improve information flows in our democratic society.

A preferred approach to news standards regulation in the digital age

A technology-neutral approach

The two recommendations put forward by the Inquiry and the Review reflect agreement that there should be a single cross-platform body responsible for news and commentary standards. This is a sound starting point in a converged media environment, where boundaries between platforms are increasingly blurred and losing their regulatory significance. Such a body would also be well-placed to adapt to future changes in the media environment, with flexibility to respond to the emergence of new platforms and delivery mechanisms.

Statutory regulation vs self-regulation

Beyond this, the conversation becomes more controversial. What level of regulatory control should this body have across all media platforms? There are two main options: move the traditionally highly regulated broadcast news and commentary into a self-regulatory structure together with print and online media, or make print and online media subject to statutory regulation.[15] Each has its critics.

There are two main options: move the traditionally highly regulated broadcast news and commentary into a self-regulatory structure together with print and online media, or make print and online media subject to statutory regulation

The Inquiry advocated the latter option; cross-platform statutory regulation. In international terms, this would be a strong and decisive outcome, certainly stronger than the current situation in Australia, or in Britain.[16] This proposal though has attracted heavy criticism from media figures, including News Limited CEO Kim Williams, who labels it "preposterous."[17] "It can never be the role of government regulators to oversee editorial positions," he argues, seeing the recommended News Media Council as a "grave threat to press freedom."[18] Williams raises a valid concern that must be considered whenever statutory regulation of media is proposed; the danger of undue political influence if the regulatory body is not constituted with a high level of government independence, and the risk that a future government could influence such a body to suppress or bypass legitimate media scrutiny. This is to be avoided in a democracy, where the media is the primary source of information for the people's political decision making. But is the risk of political influence in such a body really as great as media figures are portraying? Would it not be possible to retain an independent

11 See for example, the West Australian in 2012.

12 Parliament of the Commonwealth of Australia, report by the Senate Select Committee on Information Technologies, In the Public Interest: Monitoring Australia's Media, April 2000, (accessed 17/01/2013), http://www.aph.gov.au/senate/committee/it_ctte_completed_inquiries_1999-02/selfreg/report/a01.pdf

13 APN News & Media, Submission to the Independent Media Inquiry, 2011, 1; Submission to the Independent Media Inquiry, 2011, 3; Newspapers Publishers Association, Submission to the Independent Media Inquiry, 2011, 22; Seven West Media, Submission to the Independent Media Inquiry, 2011, 8; Finkelstein, above n 1, at 147.

14 French v Herald and Weekly Times (2010) 27 VR 171, cited in Finkelstein, above n 1, at 152.

15 These two options were each identified in the Convergence Review.

16 For example, Britain's Press Complaints Commission is a non-statutory industry body.

17 The Australian, "News to challenge media regulation", 13/07/2012, online, accessed 11/01/2013, http://www.theaustralian.com.au/media/news-to-fight-media-regulation/story-e6frg996-1226425441232

18 Ibid.

regulatory structure while eliminating the potential for government influence over the body? The Inquiry clearly states that the government would have no role in the body, apart from providing partial funding. If the government has no role in terms of appointments, the scope for undue political influence would be limited. Even if there were to be an element of political influence over the decision making of that body, its contemplated role is limited. It is not a pre-censorship body, designed to review articles prior to publication and prevent them from ever being published or to pre-empt the editorial process in any way. It is simply designed to promote responsible journalism pre-publication and offer practical post-publication options for redress on inaccuracy, unfairness and related issues, to complement the functions of parallel laws like the law of defamation and deliver more practical outcomes for victims of media inaccuracies, thereby saving time and money for complainants and media publishers in the process. The APC is already supposed to be doing this, but it has not been altogether effective.

To offer any chance of success, the new self-regulatory body would have to be actively structured in a way that promotes independence from the influence of large media organisations

Conversely, if the power of the media in influencing political decision making for voters is so great that even the remote possibility of government influence is reason enough to oppose statutory regulation (as news media organisations have argued) then that same power makes a strong regulator with the necessary "teeth" to enforce standards of accountability, accuracy and transparency against a powerful core of media organisations vitally important in a media market with one of the highest levels of ownership concentration in the world. This raises the question as to whether a pure self-regulatory structure, while removing the threat of political influence entirely, could be sufficiently strong and independent of its financial sponsors to hold them accountable for the content they produce, and guarantee the desired level of quality in Australian news standards. The history of the APC would suggest that the answer to this question is no.

Striking a balance: self-regulation with statutory reserve powers

As a result, the Review sought to strike a balance between self-regulation and statutory regulation by recommending that a cross-platform self-regulatory structure enforce standards for all news and commentary, supported by a statutory reserve power for the news communications regulator to set standards. This position acknowledges that self-regulated bodies have not been wholly effective in the past, but also seeks a compromise with industry, allowing industry to demonstrate the effectiveness of platform-neutral, self-regulatory arrangements with the threat that government will step in if self- regulation is ineffective.

At first glance, this may seem like a futile exercise. After all, 36 years of APC history have exposed the weaknesses of news content self-regulation, raising issues of media accountability. To offer any chance of success, the new self-regulatory body would have to look very different from the APC, and be actively structured in a way that promotes independence from the influence of large media organisations. The Review went some way toward this goal, recommending that the body would be run by a board of directors, a majority of whom would be independent from the members of the industry. The Review also recommended that the body wield stronger powers, including a flexible range of remedies and credible sanctions, not dissimilar from those proposed for the Inquiry's statutory body, including the power to order members to prominently publish the body's adverse findings on a relevant media platform.

These steps are encouraging, but may not be sufficient to ensure true media independence, particularly when all funding for the body is provided by industry and some of the body's directors may owe their allegiances to large media organisations. As a minimum, a preferable structure would be one in which all Directors of the non statutory regulatory body are independent from the media organisations which the body is appointed to regulate. This would likely be an unpopular position with industry, but is a necessary measure if the body is to be a truly powerful force in regulating news content and ensuring quality, accurate and transparent reporting. With this safeguard in place, a non-statutory regulatory body, which engages with the media industry in developing appropriate standards and enforcing them, is perhaps to be preferred over a statutory body which would be imposed upon the vast majority of media organisations against their will.

Who should be regulated?

In a vibrant and diverse media ecosystem, the regulatory imposition of news content standards might vary "depending upon the media involved and the extent to which they represent the mainstream media voice."[19] In this regard, the Inquiry set a low threshold, proposing that the regulator should have jurisdiction over any publisher that distributes more than 3,000 copies of print per issue or a news internet site with a minimum of 15,000 hits per year. These are admittedly arbitrary figures that have attracted much criticism for expanding the regulatory net too far beyond the mainstream.

The Review proposed a higher threshold which would apply mandatory standards to Content Service Enterprises that bring in more than $50 million of revenue a year from professionally produced local content and reach more than 500,000 Australians a month, while also allowing for "content providers that are not of sufficient scale and scope... to opt in to the relevant obligations, or to seek accreditation as a provider that has robust and transparent self-regulatory arrangements" to "enhance the brands of such providers."

In the context of an increasingly competitive multi-platform media environment, there is much to be said for an approach that incentivises membership to an industry standards body for smaller news publishers. As Hitchens explains:

> "for the blogger, citizen journalist, or the small independent online journalism endeavour, adherence to the code [or other standards imposed by the regulatory body] could in fact become a marketing or promotional tool. Unlike the established media that is able to trade off reputations established through other delivery platforms, gaining a presence and an identity may be more difficult for the independent sector".[20]

The idea of setting a high threshold for mandatory subscription, and incentivising the smaller organisations to voluntarily submit to the Code, is an elegant solution in this environment.

In order for this to work in practice however, three elements of the scheme must be calibrated. First, the mandatory threshold must be set at an appropriate level to ensure that media services

19 Hitchens, above n 3, at 233.

20 Ibid.

with substantial potential to influence the public are subject to mandatory standards. Second, voluntary membership must have the appropriate cost / benefit characteristics to make membership attractive for small and medium publishers who fall below that mandatory threshold. Third, the standards required by the scheme must encourage responsible journalism but should not be so onerous that they unnecessarily burden a publisher's ability to do business, regardless of size.

On the first point, the Review arguably sets the bar too high. A publisher does not need to generate $50 million a year in revenue from professional content in order to wield substantial influence in Australia, nor does it need to reach 500,000 Australians a month. A specialised news blog focusing on a niche industry may reach only 100,000 Australians a month and produce minimal revenue, but may have substantial ability to influence its target industry and the lives of those who participate in it. Loyal blog readers from the industry may not care whether the site has accreditation with a regulatory body, providing little incentive for the blog owner to pay a membership fee to join the regulatory body. And yet its power may be significant; factual inaccuracies published on such a blog could ruin somebody's professional image, if not corrected. This is one scenario where the proposed regulatory structure could be extremely effective in requiring mandatory compliance.

On the second point, membership fees for the body should be built around a tiered structure, based on characteristics such as revenue and monthly or annual audience, so that small and medium publishers are not at a structural disadvantage if they are required to, or elect to, join the scheme. A level of government funding may be required in order to ensure fees can be set at an appropriate level for all member organisations, so that all media organisations, whether large or small, are not disadvantaged by membership of the regulatory body. A level of government funding would be justified on the basis that high media and news reporting standards are a public good from which all citizens derive a benefit.

Finally, the standard required under codes imposed by the regulatory body should not be so onerous that they overly burden media organisations, and could also follow a tiered structure based on a publisher's revenue and audience size. Standards should be developed in consultation with the industry, bearing in mind that the primary aim of the regulation is not to require organisations to develop a new, costly and complex system of internal checks and balances prior to the production of news content; it is to encourage responsible journalistic behaviour from the outset, including appropriate due diligence and fact checking, and then effective post-publication correction mechanisms to quickly and inexpensively deal with any failures or errors. This should not impose any undue burden on news media organisations, which are in the business of providing quality journalism. In fact, established news media organisations should welcome a more extensive self-regulatory system that encourages their smaller and more manoeuvrable competitors across multiple platforms to embrace the journalistic standards that they claim to have held for many years, levelling the playing field and promoting quality news content across all platforms and publishers.

Conclusion

Just as the media environment has undergone radical changes in recent years, so too the regulatory environment must adapt to ensure strong news media standards in a modern converged media environment. The new model for news content regulation must allow media companies, large and small, to adapt to difficult and transitory market conditions and adequately preserve freedom of press which is so vital in a working democracy, while supporting quality, accurate and transparent journalism that Australians can depend on, now and in the future.

Such a model should be technology-neutral, built around a centrally managed cross-platform non-statutory regulatory body. That body should be funded primarily by industry, but with supplementary government assistance if necessary to ensure that as many media organisations as possible can afford to participate in the scheme. Otherwise the body should be completely independent from government and free from its influence. Its directors, although engaging with the media industry to develop relevant standards, should similarly be free from the influence of the media organisations they regulate, in order to ensure the regulatory body delivers an appropriate level of public accountability. The standards imposed by this body should be reasonable, not unduly onerous and determined in consultation with industry, to ensure that the scheme does not pose unnecessary financial challenges for Australian media organisations while they continue to adapt to the changing market forces and dynamics of a converged media ecosystem. Should the body fail in its purpose in some respects, as the APC has done, statutory reserve powers should be available to ensure appropriate standards are upheld.

The Government response to recent proposals of the Inquiry and the Review remains to be seen. Given the hostile reception many of the recommendations have received from large media organisations, significant progress is unlikely in this election year. Perhaps the outcome, when it does eventuate, will be a mere shadow of the bold regulatory regimes proposed in the Inquiry and the Review. Regardless, it is encouraging to see analysts, regulators and large media organisations alike remaining conscious of the importance of responsible journalism across platforms and delivery methods in today's diverse media ecosystem, and of the imperative to ensure our regulatory structures provide the right incentives to support this noble endeavour, now and in the future.

Jarrod Bayliss-McCulloch is an Associate in the Technology, Communications and Commercial (TCC) group at Baker & McKenzie. He previously completed a Bachelor of Commerce and Bachelor of Laws (Honours) from Monash University.

*This paper was awarded second prize in the CAMLA Essay Competition.

Anonymity and the Law: "The Darknet Rises"

Felix Ralph examines the challenges that the anonymity of the "darknet" poses for the legal system, copyright holders, the community and human rights.*

The darknet

Completely anonymous and encrypted browsing has the capacity to change nearly *all* current communication, media and copyright law. By rendering the internet untraceable, the "darknet" makes the law, in its current form, virtually unenforceable.

The concept of the darknet is both revolutionary and simple. It can be thought of as a series of unsearchable networks ranging from the simple copying of hard-drives between friends, all the way to a complex eco-system of layered anonymous networks.[1] Due to its nature, the size of these networks is unknowable but the regular internet is usually described as the mere tip of the iceberg in comparison to the darknet(s). The biggest of which is The Onion Routing (the ***TOR***) program. It scrambles data through various nodes to protect the IP addresses and data packets from unwanted traffic analysis. Effectively, *no-one* but the user can identify where and what content is being consumed.

The digital dilemma then deepens, with the paradox for users being that the more they desire online privacy the less they are likely to get.

The uses for the anonymity provided by the darknet can be at once noble and sinister. Cyber-criminals have adopted the network as their own. It has become a haven for child pornography and ordering drugs online.[2] All this is supplemented by an anonymous currency system that is used to finance some of these operations.[3] Conversely, the TOR network has been vital to journalists in repressive regimes.[4] Any *legally* created content on the darknet has been anonymously leaked onto the network, blatantly breaching copyright law. The TOR network has been simply described as "similar to using a twisty, hard-to-follow route in order to throw off somebody who is tailing you — and then periodically erasing your footprints."[5] What users do with their anonymous road is as diverse as the human condition.

While it does not guarantee absolute anonymity, TOR makes traffic analysis virtually unfeasible. Combined with periodic wiping of the hard drive,[6] it is almost impossible to determine the identity and location of the end-user. This means the proposed data retention policies[7] become meaningless and untraceable. As early as 2002, a number of Microsoft engineers made the simple but bold prediction that, "ultimately the darknet-genie will not be put back into the bottle."[8] Website owners do not even know who is looking at their website. Because the data is scrambled, questions of intermediary liability[9] also become moot, as internet service providers (***ISPs***) cannot hold any meaningful data. If *Roadshow Films Pty Ltd v iiNet Ltd* (2012) AJLR 494 (***iiNet case***) shows us anything, it is that the current status quo for legal enforcement of internet law relies on the dubious co-operation of the ISPs.[10] If the darknet becomes popular, the main challenge posed by this disruptive technology is the denial of *all* identifying information to ISPs, or any third party, which makes the law even harder to enforce. As always, technology spurs and requires the law to adapt to rapid changes.

One of two paths

It is not often that we stand at the precipice of great change. Technology is forcing the hand of our society to consider something that we have not experienced before; the prospect of completely anonymous community interaction. Communications, media, copyright and even criminal law must be nimble enough to adapt to this anonymous future. Essentially there are two paths we can take. The first path is one of prohibition. However, suggestions that the darknet be taken down may be ineffective. Not even considering the practical difficulties,[11] laws of prohibition may also be *ultra*

1 Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, "The Darknet and the Future of Content Distribution" *Microsoft Corporation* (2002) 1, 3. < http://msl1.mit.edu/ESD10/docs/darknet5.pdf>.

2 Geoffrey A. Fowler 'Tor: An Anonymous, And Controversial, Way to Web-Surf', *The Wall Street Journal* (Online) 17 December 2012; < http://online.wsj.com/article/SB10001424127887324677204578185382377144280.html> Editorial, 'Anonymous marketplace: software a boon for criminals and the 'darknet', The Age, (Online) 9 March 2012 http://www.smh.com.au/technology/security/anonymous-marketplace-software-a-boon-for-criminals-and-the-darknet-20120309-1uo4d.html>.

3 Bitcoin, *About Bitcoin* <http://bitcoin.org/about.html> 19 January 2013.

4 Ian Shapira, 'U.S. funding tech firms that help Mideast dissidents evade government censors', *The Washington Post* (Online), 9 March 2011 < http://www.washingtonpost.com/wp-dyn/content /article/2011/03 /09/AR2011030905157.html>.

5 The TOR Project, *TOR Overview* <https://www.torproject.org/about/overview.html.en> 19 January 2013.

6 See generally, Tails: The Amnesic Icognition Live System *About,* <https://tails.boum.org/> 19 January 2013.

7 Attorney-General's Department, 'Carrier-Carriage Service Provider Data Set' (Consultation Paper No 1.0), 2010 Commonwealth of Australia. < http://images.smh.com.au/file/2010/07/23/1710367/Secret-Document.PDF> Note: Document is heavily redacted and undated.

8 Biddle, England, Peinado, and Willman, above n 1, 1.

9 See *generally,* Roadshow Films Pty Limited v iiNet Limited (2011) 194 FCR 285.

10 David Lindsay, 'Liability of ISPs for end-user copyright infringements: The first instance decision in Roadshow Films Pty Ltd v iiNet Ltd (No 3)' (2010) 60 *Telecommunications Journal of Australia 29.*

11 See the defeated Bill, US Congress House, *Stop Online Piracy* Act H.R. 3261, 112th cong., 1st sess. (October 26, 2011).

If digital copyright owners are forced into adopting DRM systems, the role of the law should be to stand behind the rights of those owners without compromising the privacy of its citizens

vires. Like the internet the darknet is not used solely for nefarious purposes. It is also a forum for the free exchange of political, social and philosophical ideas. If legislatures attempt to impose a blanket ban on this new space it could fall afoul of the implied freedom of political communication found in the structure and text of the Constitution.[12] However, laws banning an entire medium of communication have never appeared before the High Court. The cases of *Nationwide News Pty Ltd v Wills* (1992) 177 CLR 1 and *Australian Capital Television Pty Ltd v Commonwealth (No. 2)* (1992) 177 CLR 106 only address what can be said *within* a medium, not the banning of the medium itself. Nevertheless, a law prohibiting the darknet may violate the test in *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520 which rules unconstitutional any law that effectively burdens freedom of communication about government or political matters either in its terms, operation or effect. Furthermore, such a sweeping law may not be compatible with representative and responsible government and may not be appropriate or adapted.[13]

So we are left with the second path; accepting and adapting to the changes brought by technology. If anonymous browsing becomes the norm this poses enormous challenges to artists and copyright owners. Because anonymous browsing has the capacity to circumvent legal detection, it significantly undermines the twin foundational pillars of copyright law. The first pillar is the idea that the work of the author has attached to it certain rights in property and contract. The second pillar is the utilitarian idea that copyright law, by protecting authors' rights, provides an incentive for the creation of literary and artistic works.[14] Without the protection of copyright, the artistic health of our society weakens.[15] Exclusively legal solutions have so far proved ineffective. The boom in piracy comes despite every lawsuit against a P2P network entrepreneur being successful.[16] A perfect illustration is Pirate Bay, one of the largest torrent sites, which proudly publishes expletive-riddled replies to the numerous legal threats they receive. In riposte to the multinational law firms they end with a statistic: "… 0 torrents has [*sic*] been removed, and 0 torrents will ever be removed."[17]

Despite large fines to users, legal threats are barely having an impact on the boom.[18] Any response to the problem of online pirating must take into account the old lessons taught by the P2P lawsuits when responding to new frontiers like the darknet.

The hidden dilemma

The piracy boom has created a dilemma for copyright holders. Charles Clark broadly formulated a solution to this "digital dilemma"[19] by finding that the "answer to the machine is the machine."[20] Technological innovation makes it possible to create an encrypted-lockbox embedded within content that only opens for an authorised user. This self-enforcing technology is a form of digital rights management (***DRM***) which can "directly impose technological controls on what users may, or may not, do with digital content."[21] There are multiple ways to achieve this; either through encryption, or watermarking and tracking technologies. One example is Cinavia, which embeds code into the audio of a Blu-Ray file and then limits copy and use on certain machines.[22] A stronger version of such a technology would solve the problem of anonymous browsing because copyright holders are not monitoring the traffic data of users but instead the *use* of their products. An anonymous browser still needs to download the content to use it.

It is time that we step away from the legal fiction that copyright owners are going to always be able to pursue illegal users of their content

This approach is not without its problems. Lindsay and Ricketson warn that there could a "technological arms race" between copyright owners and creators of circumvention techniques.[23] They also explore a more disturbing possibility that

> "…unconstrained implementation of technological forms of protection, such as encryption, may result in inefficiencies in the form of rent-seeking behaviour by copyright owners pursuing more returns than are available under copyright law."[24]

While TOR may protect *browsing,* it does not protect the end-users from content on their machines. The business models of compa-

12 Commonwealth of Australia Constitution Act 1900 (Imp) ss. 7, 24, 68 and 128.

13 cf: Coleman v Power (2004) 220 CLR 1.

14 Andrew Kenyon & Megan Richardson, New Dimensions in Privacy Law: International and Comparative Perspectives (Cambridge University Press, 1st ed, 2006) 125.

15 William Uzgalis, "John Locke", The Stanford Encyclopedia of Philosophy (Fall 2012 Edition), Edward N. Zalta (ed.) <http://plato.stanford.edu/archives/fall2012/entries/locke/> 20 January 2013.

16 Rebecca Giblin, *The Code Wars: 10 Years of P2P Software Litigation* (Edward Elgar Publishing Inc, 2011) 1.

17 The Pirate Bay, <http://thepiratebay.se/legal> 21 January 2013.

18 *Sony BMG Music Entertainment v Tenenbaum,* 93 USPQ 2d 1867 (D Mass, 2009); *Sony BMG Music Entertainment v Tenenbaum,* 2010 WL 2705499, at 3 (D Mass, 2010) cited in Giblin, above n 16, 2 -3.

19 United States, Committee on Intellectual Property Rights and the Emerging Information Infrastructure, *The Digital Dilemma* (Washington, DC: National Academy Press, 2000) cited in David Lindsay and Sam Ricketson 'Copyright, Privacy and DRM' in Andrew Kenyon & Megan Richardson (eds), *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge University Press, 1st ed, 2006) 128.

20 Ibid citing Charles Clark, 'The Answer to the Machine is the Machine' in Bernt Hugenholtz (ed.), *The Future of Copyright in a Digital Environment: Proceedings of the Royal Academy Colloquium* (The Hague: Kluwer Law International, 1996).

21 Ibid 148.

22 Cinavia, *What is Cinavia Technology and What does it Do?* <http://www.cinavia.com/languages/english/pages/technology.html> 21 January 2013.

23 Lindsay and Ricketson above n 19, 131.

24 Ibid.

nies like Facebook and Google rely on how much private data they can collect. In the digitised epoch, data is money. Users may turn to the darknet in droves if and when they realise the moral hazards from multinational corporations who collect their private information.[25] If this happens and users flock to the darknet, if the current trend toward pirated films continues, it would result in intolerable conditions for copyright owners. They would have no means of enforcing their rights and would be unable to pursue intermediary liability against ISP providers. The defence in the *iiNet* case becomes even stronger in the context of widespread anonymity. Thus copyright owners may be forced to implement DRM systems that increase the "use of surveillance systems by both public and private sector entities, with possibly worrying consequences for ever more rationalisation and normalisation, and the threat of increased social conformity."[26] The digital dilemma then deepens, with the paradox for users being that the more they desire online privacy the less they are likely to get.

The new role for the law is to protect the digital environment for both copyright owners and internet citizens

The new role of the law

If digital copyright owners are forced into adopting DRM systems, the role of the law should be to stand behind the rights of those owners without compromising the privacy of its citizens. This requires consideration of both copyright owners and the privacy of end-users. To protect copyright owners, liability should be incurred for the possession of software or code, which has the dominant purpose of circumventing DRM-protected products. It then falls within the responsibility of copyright owners to create digital strong boxes to protect against modern day internet banditry. Copyright owners could then request or pursue ISPs that host content that circumvents DRM systems. While this may seem like an ineffective measure for the darknet, ISPs that run illegal websites can always be contacted to shutdown those sites. It is up to the legal system to create the regulatory eco-system that protects the rights of copyright-holders. It is time that we step away from the legal fiction that copyright owners are going to always be able to pursue illegal users of their content. The key to fighting online privacy is to layer protection after protection on the content *itself,* with the law providing the regulatory framework to protect that security.

To ensure the end-users privacy, laws should be enacted that prevent DRM protected products from exceeding their original purpose of protecting the product. That is, the "rent-seeking behaviour" [27] that Lindsay and Ricketson warned against should be regulated. Such a law should allow digital *protection* of the product but not the *tracking* or *collecting* of any data received. Any tracking of data should require the clear and informed consent of the end-user. This would allow for the creation digital eco-systems that allow users to pay subscription fees for access to content. It is perfectly possible to have an eco-system that protects the rights of copyright owners and the privacy of end-users. This makes sense both from privacy *and* economic standpoints because copyright industries are most profitable "when their primary focus [i]s not to minimize unauthorized uses but rather to maximize authorized use."[28] The legal system should remove the temptation to use DRM systems to collect, survey and retain personal information and data.

To supplement these laws the definition of "personal information" in the *Privacy Act 1988* (Cth) must be broadened. Personal information is currently defined as information, "…about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion."[29]

Under this definition information that reveals the location of a user falls outside the statutory definition of personal information, but it certainly falls within a common sense definition of privacy. Such gaps need to be closed in order for citizens to have a reasonable expectation of privacy, and for governments to comply with human rights legislation.[30]

Essentially, the "machine" will correct itself. If copyright industries protect the *product* then the economics of supply and demand will take over. The new role for the law is to protect the digital environment for both copyright owners and internet citizens.

Where law and anonymity meet

It is naïve to assume that the darknet will remain a reserve for hard-core tech-heads *ad infinitum*. All parties need to begin thinking towards ways of adapting to our anonymous future. Our legal system is robust enough to change with this future *without* sacrificing the ideals that underpin it. If the law can strengthen the protection of content while broadening the privacy of users, both the interests of corporations and the rights of individuals become protected.

The darknet is not synonymous with crypto-anarchy. This paper has attempted to show that it is possible to have a thriving copyright industry, freedom of speech and communication and online anonymity at the same time. An anonymous future does not have to be an immoral one.

Felix Ralph is currently studying under full scholarship at the Victorian College of Law. He has a particular interest in criminal law and the challenges posed by new trends and technologies to the rule of law.

* This paper was awarded third prize in the CAMLA Essay competition.

25 Rana Foorahar, 'Learning to Hate Big Tech', *Time Magazine,* (New York), 4 May 2012.

26 Lindsay and Ricketson, above n 19, 147.

27 Ibid 131.

28 Daniel J. Gervais, *Collective Management of Copyright and Related Rights* (The Hague: Kluwer Law International, 2010) 17, cited in Giblin above n 16, 182.

29 Privacy Act 1988 (Cth) s 6.

30 E.g. *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 13.

The Costs of Data Retention

Nikki Macor considers the implications of proposals for wide-sweeping data retention laws on carriers.

The *Cybercrime Legislation Amendment Act 2011* (Cth) amended Australia's telecommunications legislation to facilitate Australia's accession to the Council of Europe Convention on Cybercrime, by enabling certain domestic agencies and the AFP to require that carriers preserve certain stored communications. This data preservation regime is relatively limited, requiring that agencies issue a preservation notice only where, among other requirements, access is intended to be obtained by a warrant. Communications are only required to be preserved for a maximum of 90 days or over a month-long period. The main impact on carriers, aside from a limited increase in storage requirements, is likely to be the need to ensure routine data destruction procedures allow for data subject to a preservation notice to be retained for the requisite period.

However, the government does not intend to stop at a limited data preservation regime. As outlined in the article 'Telecommunications data retention: a step in the right direction?' in this issue, the government is considering the introduction of a much broader communications data retention regime, which could require retention of data for up to 2 years.

The fundamental public policy behind both the data preservation regime and the proposed data retention regime is focused on ensuring Australian law enforcement and intelligence capabilities are adequate to deal with the ever-increasing threat posed by cybercrime.

But how will these requirements affect stakeholders? The submissions to the Parliamentary Joint Committee on Intelligence and Security inquiry (***Inquiry***) provide valuable insights into the industry's concerns.

Cost

One of the most vexing issues for industry stakeholders is the cost of establishing infrastructure to meet proposed data retention requirements.

iiNet's Chief Regulatory Officer made a statement to the Inquiry quoting a rough calculation of $60 million for start up costs for two years data storage, which would equate to approximately $400 million for the whole industry, if source and destination IP addresses are included in the scope of data required to be stored.[1] He also noted the industry's understanding that the government intends to reimburse only the actual cost of the data requested from time to time. Invariably the additional costs will be passed on to consumers, at a rate estimated by iiNet to be around $5 per month.

The Australian Mobile Telecommunications Association and Communication Alliance (the ***Associations***) cited set up costs of $500 million to $700 million and noted that any additional data element could add tens of millions of dollars to set up costs.[2] It observed that in some European countries where data retention regimes are in place, capital and operational costs incurred in compliance are reimbursed by the government, and called for the same to occur in Australia.[3]

Processing burden

Many submissions raised concerns about the onerous processing activities required to store and manage specific data sets in large volumes.

Telstra's concerns were focused on the burden of processing and managing large data sets.[4] In its view, the requirements would involve the inspection, identification and extraction of required communications data, and that this would expand its role inappropriately into communications interception.

The fundamental public policy behind both the data preservation regime and the proposed data retention regime is focused on ensuring Australian law enforcement and intelligence capabilities are adequate to deal with the ever-increasing threat posed by cybercrime

Optus, among others, raised the impracticality of effectively searching records to locate information sought by law enforcement agencies, given the sheer volume of data to be retained.[5] The Internet Society of Australia[6] also noted the additional labour force requirements that feed into the cost implications discussed above.

Security

Data security is an increasingly sensitive issue and the damage caused by breaches is constantly growing as more information is stored and transmitted electronically, and accordingly security was one of the other main issues raised by stakeholders.

Tim Berners-Lee, who is generally recognised as one of the founders of the internet, has described the data that would be stored under the proposed data retention regime as 'dynamite'.[7] He expressed doubts as to the ability of the government to keep the information secure and described what would be available to hackers as 'dossiers' of information on individuals. This highlights the importance of ensuring rigorous security over the data retained, which will amount to two years' worth of information about the communications of the nation.

---

1 S Dalby, Commonwealth Parliamentary Joint Committee on Intelligence and Security, 27 September 2012.

2 The Australian Mobile Telecommunications Association and Communication Alliance, Submission No. 114, Parliamentary Joint Committee on Intelligence and Security, [3.47].

3 The Australian Mobile Telecommunications Association and Communication Alliance, Submission No. 114, Parliamentary Joint Committee on Intelligence and Security, [3.45].

4 Telstra, Submission No. 189, Parliamentary Joint Committee on Intelligence and Security, p11.

5 Optus, Submission No. 206, Parliamentary Joint Committee on Intelligence and Security, p3.

6 Internet Society of Australia, Submission No. 145, Parliamentary Joint Committee on Intelligence and Security, p3.

7 Lateline, 29 January 2013, (available at: http://www.abc.net.au/lateline/content/2013/s3679053.htm).

As the government will not be storing the majority of the data, the standards by which carriers and carriage service providers will store and recover data will be critical to maintaining the security of the treasure trove of information. As noted by the Internet Industry Association, it is not yet clear what standards will be imposed,[8] but what is clear is that higher standards will lead to higher costs.

Competitiveness

Submissions identified potential issues for competitiveness at both domestic and international levels.

The Internet Industry Association explained that increased costs imposed on Australian services may result in them suffering a competitive disadvantage against offshore 'over-the-top' services such as Gmail.[9] Offshore providers are already dominant, and any reduction in the competitiveness of the Australian industry would merely reinforce and exacerbate this situation.

The Internet Society of Australia also pointed out that domestic competition may be hampered by higher barriers to entry, given the additional costs and infrastructure requirements associated with meeting proposed data retention requirements.[10]

Privacy

The retention and availability of vast stores of personal information poses an obvious threat to privacy that was recognised in a number of submissions.

In its written submission, iiNet concluded that data retention requirements would effectively create a statutory exemption to National Privacy Principle 1.1 under the *Privacy Act 1988* (Cth), which requires that an organization not collect personal information unless the information is necessary for one or more of its functions or activities.[11]

iiNet's statement to the Inquiry raised the likelihood that the proposed data retention requirements will be extended to other fields in due course, such as transport, utilities and retailers. The Associations pointed out that the inclusion of location data of mobile telephone users could result in continuous tracking and surveillance of all mobile customers.[12]

Given the volume of information that will be collected under the data retention proposal, this could have a significant impact on privacy protections for all Australians.

Conclusion

With the recent retirement of Nicola Roxon as Attorney General, there may be some doubt as to the future of the data retention proposal. Roxon's incoming replacement Mark Dreyfus has been reported as being sympathetic to privacy concerns and it is not yet clear whether he will support and prioritise the proposal as strongly as Roxon.[13] However, as the submissions to the Inquiry indicate, if the government does proceed with the proposal, there will be significant issues to be overcome by the industry.

Nikki Macor is a lawyer at Allens. The views expressed in this article are the views of the author only and do not represent the views of any organisation.

---

8 Internet Industry Association, Submission No. 187, Parliamentary Joint Committee on Intelligence and Security, p8.

9 Internet Industry Association, Submission No. 187, Parliamentary Joint Committee on Intelligence and Security, p8.

10 Internet Society of Australia, Submission No. 145, Parliamentary Joint Committee on Intelligence and Security, p3.

11 iiNet, Submission No. 108, Parliamentary Joint Committee on Intelligence and Security, p12.

12 The Australian Mobile Telecommunications Association and Communication Alliance, Submission No. 114, Parliamentary Joint Committee on Intelligence and Security, [3.48].

13 C Porter, news.com.au, 4 February 2013 (available at: http://www.news.com.au/technology/mark-dreyfus-not-ruling-out-data-retention-spy-plan/story-e6frfro0-1226570198350); J Gliddon, itnews, 4 February 2013 (available at: http://www.itnews.com.au/News/331094,data-retention-stalls-at-committee-level.aspx).

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 hard copy and electronic format and comments should be forwarded to the editors of the Communications Law Bulletin at editor@camla.org.au or to

Valeska Bloch or Victoria Wark

C/- Allens
Deutsche Bank Place
Corner Hunter & Philip Streets
SYDNEY NSW 2000

Tel: +612 9230 4000
Fax: +612 9230 5333

Please note the change to CAMLA contact details:

Email: camla@tpg.com.au
Phone: 02 9399 5595
Mail: PO Box 237,
KINGSFORD NSW 2032

THE UNIVERSITY OF MELBOURNE

MELBOURNE LAW SCHOOL

The Melbourne Law Masters 2013

Melbourne Law School – Australia's number one and world number eight law school in the 2012 QS World University Rankings.

www.law.unimelb.edu.au/masters

Australia's first, Australia's global.

Communications & Media Law Association Incorporated

The Communications and Media Law Association (**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 & on-line services

In order to debate and discuss these issues CAMLA organises a range of seminars and lunches 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 (**CAMLA**) 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.

CAMLA Website

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

Application for Membership

To: The Secretary, camla@tpg.com.au or CAMLA, Box 237, KINGSFORD NSW 2032
Phone: 02 9399 5595

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:

☐ I Ordinary membership $130.00 (includes GST)

☐ Corporate membership $525.00 (includes GST)
(list names of individuals, maximum of 5)

☐ Student membership $45.00 (includes GST)
(please provide photocopy of student card - fulltime undergraduate students only)

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