Communications Law BULLETIN

CAMLA

Communications & Media Law Association Incorporated

Print Post Approved PP: 234093/00011

# Facebook - Advertiser Liability For User Comments… A Post Too Far?

**Linda Luu and Alison Willis consider two recent determinations by the Australian Advertising Standards Bureau concerning the liability for the posting of user comments on an advertiser's Facebook sites.**

## Introduction

In two recent landmark case reports,[1] the Australian Advertising Standards Bureau (***ASB***) has determined that user comments on an advertiser's Facebook site are an *'advertising or marketing communication'* as defined in the Advertiser Code of Ethics (the ***Code***). In one of these decisions, an advertiser was also held liable for the user comments.

As a result, not only will advertisers in Australia be held responsible for content generated by or on behalf of themselves on their own Facebook site, but also for material or comments posted by users or friends. In practice, this requires advertisers who have Facebook or similar social media sites to regularly monitor user comments and remove posts which may breach provisions of the Code.

This determination has serious implications for advertisers that engage in social media or other interactive advertising. This article analyses these decisions and considers their implications for the increasing number of businesses which make use of social media. The authors also consider whether the Code is properly equipped to deal with new forms of communications such as social media.

## ASB determination

On 11 July 2012, the ASB published two case reports in response to a single complaint made in relation to user comments posted on both the official VB and Smirnoff's Facebook sites (owned by Fosters Australia, Asia & Pacific, part of Carlton United Brewers (***CUB***) and Diageo Australia Ltd[2] respectively). The role of the ASB is to receive and review the merits of complaints made in relation to advertising and marketing communications and it may initiate a formal investigation based on a single complaint.

The key question to be determined by the ASB was whether the user comments on VB and Smirnoff's Facebook sites were an *'advertising or marketing communication'*, which is defined in the Code as:

- 'any material which is published or broadcast using any Medium or any activity which is undertaken by, or on behalf of an advertiser or marketer, and
- over which the advertiser or marketer has a reasonable degree of control, and

1 Case number 0271/12 (Fosters Australia, Asia Pacific) and case number 0272/12 (Diageo Australia Ltd). ASB case reports are available at http://www.adstandards.com.au/.

2 Case number 0272/12.

**Volume 31 Nº 4**
**October 2012**

## Inside This Issue:

# Contents



- that draws the attention of the public in a manner calculated to promote or oppose directly or indirectly a product, service, person, organisation or line of conduct…'

In making the determination, the ASB found that:

> '…the Facebook site of an advertiser is a marketing communication tool over which the advertiser has a reasonable degree of control and that the site could be considered to draw the attention of a segment of the public to a product in a manner calculated to promote or oppose directly or indirectly that product. The Board determined that the provisions of the Code apply to an advertiser's Facebook page. As a Facebook page can be used to engage with customers, the Board further considered that the Code applies to the Content generated by the page creator ***as well as material or comments posted by users or friends***...'[3] [our emphasis]

## This determination has serious implications for advertisers that engage in social media or other interactive advertising

The ASB found the user comments to be an advertising or marketing communication within the meaning of the Code and went on to assess whether the user comments breached the Code. A number of the particular allegations of Code breaches were upheld against Fosters but all allegations of Code breaches were dismissed against Diageo.

### Analysis of the determination

Fosters submitted that there is a distinction between comments, questions and material posted by or on behalf of advertisers and user comments. Fosters argued user comments were not an advertising and marketing communication for the following reasons:

> '…they are not material "over which [CUB] has a reasonable degree of control". While CUB has the ability to monitor and remove User Comments from the VB Page…pre-moderation by CUB of User Comments on the VB Page is not commercially feasible therefore CUB has no practical control over the content of the User Comments…pre-moderation of every User Comment would be contrary to the spirit of social media and would cause users to become disengaged from the page… Further… User Comments… are not "calculated to promote or oppose directly or indirectly a product, service, person, organisation or line of conduct"…'

1. First Limb: Does the advertiser have a reasonable degree of control?

Despite Foster's claim that it has no practical control over the user content, as the owner of the Facebook site and as acknowledged in its submissions, it does have the ability to monitor and remove user comments from the VB Page, which appears to satisfy the first limb of the definition.

2. Second Limb: Are the comments calculated to promote a product or organisation?

There are strong arguments on both sides as to whether the second limb of the definition of 'advertising or marketing communication' is or isn't satisfied. The key question to be applied is, is all dialogue in response to an advertiser post on its own Facebook site:

> 'calculated to promote or oppose directly or indirectly a product, service, person, organisation or line of conduct'?

The ASB appears to have given weight to two factors, however it did not specify these in detail in its reasoning – so we have expanded on the reasons they provided. First, the user comments are on an advertiser's Facebook site and accordingly it is compelling for the ASB to have found that the site is most likely calculated to 'indirectly promote that company'. Secondly, the user comments identified in the complaint were posted in reply to questions posted by the advertiser such as *'Besides VB, what's the next essential needed for a great Australia Day BBQ?'.* In our view it is also reasonable for the ASB to have found that responses to the questions posted by the advertiser are most likely calculated to 'promote the product'.

3 Case number 0271/12, at 7.

## How do users 'use' social media?

However, with respect to the ASB determination, we have difficulty in accepting the decision in respect of the second limb without testing. It is evident in the ASB determination that it elected not to consider the mechanics of how user comments can ultimately be posted to a Facebook site. When we posted a user comment to VB's Facebook page, that comment then appeared on all of that user's friend's newsfeeds and provided those friends with the option of also commenting on the user comment (or 'liking' it). We noted that although there is some identification of the VB Facebook site in the newsfeed, the friend can comment or 'like' the photo without clicking through to the actual VB Facebook site (only the picture and the relevant comments and 'likes' are viewable).

This is a grey area that is not addressed in the determination – whether it is fair that an advertiser is liable for comments that users have made, when those users are not even required to have visited the advertiser's Facebook page to make the comment. We acknowledge that the answer may still be yes because the advertiser benefits from having the Facebook site and is therefore fully responsible for the site. However, as considered further below, we doubt this would have been in the contemplation of the Australian Association of National Advertisers (***AANA***) in 1997 when it established the Code. Although the determination is currently confined to Facebook sites, we note that social media includes all web and mobile-based technologies which are used to turn communication into interactive dialogue among organisations, communities, and individuals.[4] This could have many more implications for other web interactions between advertisers and users.

Further, as stated above, Foster submitted that advertiser generated content and user content should be treated differently under the Code, specifically with user content being more analogous to a conversation at a restaurant or a pub.

Is user content more analogous to a conversation at a restaurant or a pub? The general public, which uses and engages in social media, would probably agree as they understand the difference between advertiser content and user content. However, there are also unsophisticated users of social media who may not understand the difference.

For the reasons set out above it is arguable that user comments themselves fall into two categories. User comments that mention VB or competitor products clearly satisfy the second limb of the definition. However a user comment such as *'is a man's job women should b chained 2 da kitchen! Lmfao'* (in response to an advertiser post about brewing being every man's dream job) is arguably part of an interactive dialogue which is not promoting the advertiser's product.

The same complaint is also due to be considered by the Alcohol Beverages Advertising Adjudication Panel against the Alcohol Beverages Advertising Code (***ABAC***), which will consider similar issues, and which has not yet occurred at the time of writing.

## Limitations of the Code

Since its inception in 1997, the Code has not been updated to address the new challenges of social media, despite the increased use by advertisers of sites such as Facebook and Twitter.

Readers will recall that the media industry in 1997 comprised traditional forms of media such as television, radio, print and billboards. Back then, advertising on the internet was in its infancy and social media was unheard of. It is now appropriate for a review of the Code to provide specific guidance for advertisers in relation to use of social media as an advertising tool.

## Allergy Pathways

Before we return to the VB and Smirnoff case, it is useful to revisit the Federal Court decision in *ACCC v Allergy Pathway Pty Ltd and Anor (No 2)*.[5] In 2009, the Australian competition and consumer protection regulator, the Australian Competition and Consumer Commission (***ACCC***), brought an action against Allergy Pathway for engaging in misleading and deceptive conduct, falsely representing that goods or services were of a particular standard or quality, or had benefits which they did not have under the (then) *Trade Practices Act* 1974 (Cth).[6] Allergy Pathway offered up undertakings to the Court to refrain from making any further misleading or deceptive publications or statements about their products and services.

**Since its inception in 1997, the Code has not been updated to address the new challenges of social media**

In 2011, the ACCC commenced separate proceedings alleging Allergy Pathway was in contempt of the undertakings because of testimonial claims posted by users of its products on Facebook and Twitter about Allergy Pathway's allergy treatment products. Allergy Pathway and its sole director were found to be in contempt because of the Facebook and Twitter statements. Key factors in the decision were that Allergy Pathway knew the statements had been posted on its Facebook and Twitter pages and did not remove them. Additionally, if Allergy Pathway had made the statements itself, it would have been in breach of the undertaking.

Finkelstein J said:

> 'While it cannot be said that Allergy Pathway was responsible for the initial publication of the testimonials (the original publisher was the third party who posted the testimonials on Allergy Pathway's Twitter and Facebook pages) it is appropriate to conclude that Allergy Pathway accepted responsibility for the publications when it knew of the publications and decided not to remove them. Hence it became the publisher of the testimonials.'[7]

While the test applied in the Allergy Pathway case is different (i.e. the test applies the first limb of the test in the Code and not the second limb), it is relevant that the user comments were testimonial claims about the relevant products (and not comments such as in the VB case which were often irrelevant to the advertiser post or to the VB products themselves).

## Implication of the cases

The consequence of the VB and Smirnoff case when viewed together with the Allergy Pathway case is potentially wide-ranging and legal observers are still considering the extent to which an advertiser will be responsible for what is posted to their Facebook sites.

One fairly dramatic example is whether individuals will be liable in the future for defamatory comments made on their Facebook pages which are not removed in a timely fashion. Obviously the contexts are vastly different but the principle is the same (given that individuals would not be responsible for the initial publication but would accept responsibility for the publications when they knew of the publications and decided not to remove them).

---

4 http://en.wikipedia.org/wiki/Social_media.

5 *ACCC v Allergy Pathway Pty Ltd and Anor (No 2)* [2011] FCA 74.

6 [2011] FCA 74, at [5]. The *Trade Practices Act* has since been re-enacted as the *Competition and Consumer Act 2010* (Cth) (***CCA***), The prohibitions on misleading and deceptive conduct and false representations are now contained in the Australian Consumer Law, which comprises Schedule 2 of the CCA.

7 [2011] FCA 74, at [33].

## The ACCC statement appears to place more stringent regulation on large companies as opposed to smaller companies

The ACCC was quick to contribute its own commentary, issuing a statement to warn large companies using Facebook to promote themselves that, *'If you are a big corporate player with lots of resources that's putting a lot of effort into social media then it wouldn't have to be too long [that corporations have to take down comments]. Perhaps 24 hours or less.'*[8]

This statement appears to place more stringent regulation on large companies as opposed to smaller companies, even though such a distinction has no basis in either the Code or the *Competition and Consumer Act* 2010. We also question whether it is fair for different advertising rules to apply to 'big' or 'small' advertisers and note there is no guidance as to what the ACCC considers a big or small company.

In response to the case report, Fosters has already implemented twice daily monitoring of user comments (in addition to removing all of the user comments that were highlighted in the complaint).[9] Of course, many large companies are already sophisticated users of social media - at an American Chamber of Commerce lunch in Sydney in July this year, Telstra's Chief Executive David Thodey revealed that Telstra employed around 60 people to monitor social media sites.

However, not every company which has a Facebook page is a large company with extensive resources. The Sensis *e-Business Report*[10] found that companies in Australia have clearly embraced social media engagement - 27% of small and medium enterprises which have internet connectivity (being 92% of all small and medium enterprises) also used social media in their business. The most common usage of social media was to have a Facebook page for their business, presumably because social media (to date) has been low cost and low maintenance. It is too early to measure the potential impact of the determination on companies which are not resourced to monitor their Facebook sites regularly.

### Will regulatory bodies in other jurisdictions follow suit?

A final point to bear in mind is that the ASB determinations apply only to advertisers in Australia. There is a possibility that advertising watchdogs in other jurisdictions may follow suit. We note that in the United States, section 230 of the *Communications Decency Act 1996* (***CDA***) provides 'computer services providers' (as defined in the CDA) with immunity in certain circumstances for publishing tortious statements (e.g. defamatory statements) online. This legislation has been successfully used as a defence by website owners such as AOL,[11], Ebay[12] and Google[13] to negate their liability for user generated content. However, at the date of this article, we are not aware of any cases alleging the liability of advertisers for user generated content uploaded on their branded social media pages.

***Linda Luu is a lawyer and Alison Willis is a consultant at Gilbert + Tobin in Sydney, Australia in the Corporate, Communications and Technology Group. The opinions presented in this article are personal to the authors and do not represent the views of any organisation or client.***

---

8 Julian Lee, 'Warning to firms on Facebook comments', *Sydney Morning Herald* (online), 13 August 2012 <http://www.smh.com.au/technology/technology-news/warning-to-firms-on-facebook-comments-20120812-242vr.html>.

9 Case number 0271/12

10 Sensis, *eBusiness Report: The Online Experience of Small and Medium Enterprises* (August 2012) 4 <http://about.sensis.com.au/small-business/sensis-ebusiness-report/.

11 *Zeran v America Online. Inc.,* 129 F. 3d 327 (4th Cir 1997).

12 *Gentry v. eBay, Inc.,* 99 Cal. App. 4th 816, 830 (2002).

13 *Goddard v. Google, Inc.,* 640 F. Supp. 2d 1193 (N.D. Cal. Jul. 30, 2009).

# Regulation in a Converged Environment

**Chris Chapman, Chairman and Chief Executive, Australian Communications and Media Authority, delivered the keynote address at the Charles Todd Oration in Sydney, on 30 August 2012.**

In 1870, as now, the world was at a then global tipping point for technologically enabled change. The innovative technology of the day, the telegraph, was seen as the 'key to prosperity and wealth' for the then still separate Australian colonies. With the building of the Port Augusta to Darwin telegraph, Charles Todd connected Australia to the world and, with that, global change.

The communication network that the telegraph established across and beyond Australia has been characterised as the 19th century equivalent to our 21st century broadband. Charles Todd refused to be tyrannised by distance and pioneered our electronic connection with the world, becoming perhaps our very first internet pioneer.

The Charles Todd oration is an opportunity to commemorate our global connectedness and celebrate the pivotal role that communications technology plays in continuing to build and shape our ever-deepening engagement with the world. And later in my oration, I'll also highlight the modern challenges we (all of us) will need to address to keep the human face of our sophisticated communications technology as simple and robust as it was in Charles Todd's day.

The ACMA conducts its diverse regulatory activities across a continent that has a number of distinct characteristics.

Our electronic connection with the world, commencing with Charles Todd's telegraph and continuing with the optical fibres and satellites of the present day, means that notwithstanding our unique Australian characteristics and circumstances, we can nonetheless equally network and interweave with and benefit from global developments, and globalisation itself.

Thomas Friedman captures the global state of play well in his latest book, *That Used to be Us: What Went Wrong With America? And How it Can Come Back*. He sees two of the great challenges facing his country (and it applies equally to ours) as firstly, adjusting to the ongoing IT revolution, and secondly, understanding and working with globalisation. He sees these, in fact, merging into one major challenge, which he calls the 'hyper-flattening' of the world.

With this hyper-flattening, many are of the opinion that we have now begun to enter what could be termed a 'hyper digital' era, combining the power of ICT with ubiquitous high-speed broadband, enhanced by analytics, semantic systems, cognitive computing, agent technology and the like.

Australia is right now building out a broadband network to engage with, and grasp the opportunities of, this future global digital world. The technological changes leading us to this point have often been described as 'convergence'. Some history is important here, as today I want to start to move the discussion forward from a focus on convergence, as we have come to understand it, to the broader and more nuanced idea of a networked society.

The ACMA was created to be a 'converged' regulator way back in 2005, designed to bring together the threads of the evolving communications universe, specifically the convergence of the four 'worlds' of telecommunications, broadcasting, radiocommunications and the internet. How breathtakingly simple that intent must have seemed.

The four core principal acts which relate to these 'worlds' – the Radiocommunications Act,[1] the Telecommunications Act,[2] the Consumer Protection and Service Standards Act[3] and the Broadcasting Services Act[4] – are now decades old and have become increasingly difficult to apply in this 'converged' …now moving towards a networked society … environment. The age of these Acts is perhaps most usefully illustrated by the observation that they were made before the internet took off in Australia.

**we have now begun to enter what could be termed a 'hyper digital' era, combining the power of ICT with ubiquitous high-speed broadband, enhanced by analytics, semantic systems, cognitive computing, agent technology and the like**

Due to the rapid changes that, as I have said, sped across our landscape, those core Acts have then been incrementally supplemented with amendments, new schedules, a range of purpose-specific Acts (such as the Spam Act 2003 or the Interactive Gambling Act 2001) or ministerial determinations. These additions have been made reactively (that is, in response to developments in such seemingly disparate arenas of hardware, software and connectivity, changing social attitudes and behaviours, enhanced citizen expectations and/or globalised economic shifts).

In the majority of cases, these changes have been 'tacked on' to existing legislative constructs (that is, those established in the core Acts). And it logically follows, for this reason, that every supplementation to a core Act is inevitably based, to some extent, on dated concepts set out in that legislation. As all of us are aware, the most recent attempt to grapple with this from a more holistic perspective was the recently completed Convergence Review. The government is currently considering the recommendations of that review before responding and so, as a portfolio team player, I proffer no pre-emptive suggestions.

Suffice it to say, however, that we at the ACMA, meanwhile, have simply been getting on with our day job while continuing to build on our informative and highly valued and cited work in the convergence space. These two threads, doing our day doggedly and relentlessly and yet bridging to the future with forward-thinking work programs such as spectrum re-farming, numbering plan reform and telco service paradigm shifts, builds a solid case of delivery on our adopted purpose; 'making media and communications work in Australia's national interest' – a sentiment that would put a smile of

1 *Radiocommunications Act 1992* (Cth).

2 *Telecommunications Act 1997* (Cth).

3 *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth)

4 *Broadcasting Services Act 1992* (Cth).

**the challenge of digitalisation has not been fully addressed legislatively and indeed this challenge appears to have been compounded by (in fact, run over by) the emergence and dominance of IP networks in the last decade**

Charles Todd's face, given his own immeasurable service to Australia's national interest.

And similarly early in my term as Chair, I set an aspirational standard for the ACMA (as a convergence-oriented organization) to be measured against in delivering on that purpose, namely:

To be, and to be recognised as, the world's best converged regulator.

I provocatively adopted this goal to stretch the organisation and to drive the ACMA towards world's best practice. The standard has been part of ACMA internal transformation and business planning activities over the last four or so years. It has been articulated externally in our annual ACMA rolling three-year corporate plan since the 2009–12 plan was published in 2008.

Because measuring converged communication regulation performance in a globally valid way is inherently problematic, we chose to take a narrative approach using descriptive case studies rather than one of meaningful measurement.

The narrative framework of our assessment captures the fundamental tasks of any regulator in a convergent environment, central to which is delivering outcomes in the public interest. I personally feel we can legitimately claim, with our current one-third assessment, to have already gone a considerable way to meeting our standard. In any event and far more importantly, I think this leaves the agency well positioned to be the future regulatory centre point for a digitally connected Australia and its evolving networked society. We have the strategic vision, we have demonstrated capability right across our bench and we have the energy to deliver on that positioning. So expect no respite from the ACMA, especially as we further live to our brand strapline of 'Communicating, Facilitating (and if all else fails) Regulating' … the 'if all else fails' bit does not actually appear in the written version of the strapline!

This notion of work in the public interest is internationally common ground. Neither Australia nor the ACMA is divorced from the globally shared imperative to come to terms with public interest issues in an environment of communications and media convergence. I earlier touched on the Convergence Review. An important, but perhaps not obvious, element of the ongoing convergence debate is that 'convergence' itself is not a stable concept.

Original concepts of convergence stemmed from digitalisation, and no more, which during the 90s broke the nexus between the shape of content and the container which carried it–'for example, a voice call was no longer solely defined by being carried on a plain old telephone network. This has meant that regulation constructed on the premise that content can be controlled by how it is delivered, or that delivery systems are defined by the user service they carry, has increasingly lost its force, both in logic and in practice.

In fact, it would seem that markets have almost totally now digested digitalisation with the ACMA, as the regulatory facilitator, playing a critical role in completing important parts of a practical digitalisation project (the switchover to digital television). However, the challenge of digitalisation has not been fully addressed legislatively and indeed this challenge appears to have been compounded by (in fact, run over by) the emergence and dominance of IP networks in the last decade. This has meant content has become increasingly non-linear, interlinked and 'uncontained' while people increasingly expect to connect and communicate seamlessly – anywhere, anyhow, anytime (I guess, when you think about it, the 21st century equivalent of Charles Todd's intent). We need to acknowledge the inevitable movement towards an even more complex communications world, where network elements can and will be emulated in software (think 'virtualisation'), leading in turn to an ever more intricate and subtle interconnection between networks, devices, services and content.

Reform of the current arrangements can perhaps aim to bring the current system 'up-to-date' with digital, and maybe grapple with the early impacts of the web. However, things have changed quite radically over the last six or so years. And I suggest we (all) must plan for further radical change over an indicative lifespan of any proposed regulatory reform process. Sitting where I sit and having daily intimate knowledge of the various influences and dynamics and their interplay with current Acts and regulatory constructs, that process needs to make use of broader concepts of convergence than those we have only just got used to, concepts that take into account the fact that we are dealing with deeply complex, indeed ambiguous, changes in communications and media today. For example, is network functionality hardware or software, is a voice-call a service or now just an app (and I will return to that query).

It seems unlikely to me that we will settle into a new agreed order or commercial equilibrium in media and communications any time soon, any more than we will be able to maintain the status quo of 'industrial' communications and media …even if we wanted to. We (and I mean here regulators and policy-makers) have almost come to terms with the concept of 'online' media as opposed to the 'offline' traditional media. This is essentially the impact of digitalisation and the first wave of IP networking, aka the World Wide Web. But that is more than a decade-and-a-half old! The split is no longer binary – 'online' has already moved on through a number of iterations.

**As access to the internet becomes ubiquitous, and the internet migrates to other platforms (such as television sets), the content regulation situation has become increasingly anomalous**

The internet is now starting to deliver on its fuller media distribution potential with the advent of always-on broadband, which is capable of delivering broadcast television (and better) quality video. The internet has also created global reach for such audiovisual material. I said a minute ago that we have almost come to terms with 'online' because developments in social networking are changing the game away from the 'online' website world as much as from the 'offline' world, as commercial content is increasingly embedded within the extensive context of social network messages and user-generated content. Commentators recently referred to the London Olympics as the first social media games …with athletes interpolating their athletic endeavours with social media PBs. This audience doesn't, but the wider audience forgets that it's a generational thing.

As access to the internet becomes ubiquitous, and the internet migrates to other platforms (such as television sets), the content regulation situation has become increasingly anomalous. Indeed broadcasting and newspaper operators are increasingly offering internet-based services to complement their other offerings. Many individuals in networks now access and link to the more persistent elements of content published to 'audiences', freely sharing their experience with others and spreading the influence not only of the original material but also adding the strength of a recommendation (positive or negative). Traditional media are now immersed in and mining the world of social media for updates and breaking news.

## Networks present a much greater regulatory challenge than linear situations such as broadcasting or simple phone calls, since the latter offer relatively easy 'points of control'

Crucially, from the traditional perspective of a public interest regulator, this network of citizens, freely expressing their views, does not have a single control point, such as a transmitter (or the equivalent of Todd's telegraph Morse code equipment) … should intervention be required. Networked media do not exert their 'influence' in a singular or directional way. Networks present a much greater regulatory challenge than linear situations such as broadcasting or simple phone calls, since the latter offer relatively easy 'points of control'. The communications and media space is continuing to evolve, and our regulatory response is simply going to need to evolve with it, including an ongoing reassessment of the pros and cons, the social good, of when intervention is required and how it is effected.

So I think this evolution drives a need to empower the regulator to be flexible and rapidly adaptive to changing industry circumstances (which may involve more rapid 'fit for purpose' intervention and may equally, if not more so, involve regulatory discretion and the exercise forbearance). This empowerment will be a crucial part of the way forward. The ACMA is not, however, just sitting and waiting for this to be done for us, or to us. Recognising and acting on these necessities in today's world, we are, as I've assured you, engaged, energetic and very much alive to the need to continuously reinvent ourselves.

Convergence in its broadest sense sits behind all the challenges and initiatives we undertake within our exceptionally broad remit, encompassed by our patchwork legislative mandate. And just to assist your powers of recall, highlights of our recent work encompass:

- the detailed preparatory work on the 700 MHz and 2.5 GHz radio spectrum to deliver the digital dividend, and our pursuit of providing substantially more broadband spectrum through a relentless program of 're-farming';
- the fresh, 'first principles' block configuration approach we have taken to the digital dividend broadcast spectrum restack process;
- our recognition of the compelling necessity for Australian citizens and consumers to be much better educated about both the opportunities of the digital economy and the threats in the online and social media worlds;
- exploration of the unchartered waters for the ACMA (and perhaps indeed for all industry participants) in 'Phase 2' of the NBN;
- energising the long overdue necessity for the telco industry's customer service and complaints-handling performance to be reset (which I will return to below); and
- our pre-emptive initiative for fresh approaches to our telecommunications numbering arrangements as the inevitability of unified communications marches on.

It is to the latter aspects of telecommunications that I will now turn, since in my view, thinking about the future of voice services is a useful lens for looking at these deep running 'convergence' changes, and one that is relevant in the context of the telecommunications legacy of Charles Todd.

Exactly a year ago, the ACMA released *Broken concepts –'The Australian communications legislative landscape,* which highlighted the ever-increasing strain on old legislative and regulatory concepts struggling with new technology, and this, along with a companion piece titled *Enduring concepts – Communications and media in Australia* neatly framed the Convergence Review's challenges. That review alluded to (although did not ultimately conclude with) an approach which focused on a 'converged structure' based on four layers – infrastructure, networks, content and applications, and devices.

I think using a layers analysis of convergence is useful for the immediate future and, as an example, it helps makes sense of the way in which voice telephony is increasingly being transformed into 'just' another user app on a smart device or within a social media context, alongside a myriad of other more or less useful apps. The vendor of the voice app can easily be substituted with another, or with another channel of communication altogether.

Such simple telephony apps could be seen as important but low-value applications running on top of existing data infrastructures, rather than as a dedicated, premium value end-to-end service. Indeed, Ovum has recently estimated that 'over-the-top' voice and messaging applications cost traditional telecommunications operators worldwide 13.9 billion dollars (or nine per cent of their revenue last year).

The nature of voice application is also growing beyond simple 'calls' and now voice communication often sits in the context of other media and ways of messaging; for example, chat between players of an online game. 'Telephone numbers', as such, are slowly losing their special place and are becoming part of the web of addressing that binds the various network layers together as that precursor of unified communications.

As companies in this space scramble (or soon will be forced to scramble) for new enduring business models, Australia once again is being inexorably enmeshed in the global.

## Your search engine knows a lot more about you than your local registry of births deaths and marriages, or the Passport Office. Maybe not more than the Tax Office – not yet anyway!

National sovereignty is under challenge, as the location of the server is currently as relevant as a person's actual physical location. The data captured outside of government becomes perhaps more potent than government, the traditional repository of information about a country's citizens. Your search engine knows a lot more about you than your local registry of births deaths and marriages, or the Passport Office. Maybe not more than the Tax Office – not yet anyway!

The heady brew of new business models, new platforms, and new forms of user interaction will continue to ferment and, as it does, will raise regulatory question marks and potentially massive challenges for government regulators intersecting with this space.

Notably, most communications services are no longer handled by one integrated entity. It is a more complex environment – a network in the new sense – and when things go wrong, it can be more difficult to identify who was responsible, what has gone wrong and in which locale the perpetrator is actually situated.

Participants in recently published ACMA research, *Digital Australians,* very interestingly, very encouragingly, confirm an awareness of the different roles that the individual, the private sector and government play to ensure that their online experience is positive. The research indicates that Australians accept their responsibility in the online environment, but they are also looking to industry and government to help them in managing that complex environment.

## The ACMA decision to register the TCP Code, is a watershed event that should shift behaviour in the telecommunications landscape

This is an abiding concern for the ACMA, and I'll turn now to an example of a very specific regulatory challenge, a microcosm if you like of the issues that arise in a networked society. Our recent public inquiry into customer service in the telco sector, known as *Reconnecting the Customer,* concluded that co-regulation had not been working effectively in the interests of consumers in an increasingly complex environment of platforms, products, services and suppliers.

Consumer complaint levels had been far too high and poor customer care (both directly and indirectly) drove many consumers to complain. We observed great complexity in the packages or bundles offered by service providers, as well as their pricing. Even from a single service provider, the task of deciding the bundle that best matches a consumer's individual preferences for type of service, quality, speed, handset and volume of usage is complex. Comparing packages across service providers is concomitantly more complicated – not only do a number of packages from each of a number of service providers have to be compared, but the information about essentially the same service is provided in different ways.

Although this complexity is generated by service providers, it partly responds to consumers' wants (for example, access to different services on one device), and it provides potentially attractive benefits for consumers, along with uncertainties and risks. It has profound impacts on the behaviour of both consumers and service providers. We found work in the field of behavioural economics particularly useful in considering ways to assist consumers navigate this complexity. We noted that consumers:

- can only take so much product information into account and are susceptible to advertising;
- are likely to copy the decisions of friends, rather than make time-consuming independent enquiries;
- are unlikely to dig deeper into fine print; and
- can be short-sighted in their purchasing decisions.

As a consequence, each of these factors increases the likelihood that a consumer will make a choice that turns out to be a comparatively poor one in hindsight and the ACMA's resultant conclusions have been designed to drive product offerings in this particular domain that are more comprehensible and help consumers avoid these and other behavioural traps. It is an aspect of human behaviour by people, both as consumers and citizens, that will need to inform the possible evolving interventions in other complex areas of media and communication.

In the ACMA's final inquiry report, we also noted that this so-called 'bounded rationality' is no criticism of the behaviour of consumers or citizens, but merely describes the findings of current empirical research in behavioural economics.

One important outcome from that inquiry has been guidance to the formulation of a vastly improved Telecommunications Consumer Protections Code (the **TCP Code**). The ACMA decision to register the TCP Code, is a watershed event that should shift behaviour in the telecommunications landscape.

It provides a comprehensive set of enforceable safeguards for Australia's telecommunications consumers. All of the primary protections are contained in a single document and the protections are aimed at addressing key points in the customer/provider lifecycle. In other comparable markets such as the USA, the United Kingdom and New Zealand, there is no single telecommunications instrument of consumer protection or of such magnitude.

The telegraph for which Charles Todd is so justly famous, while unquestionably advanced for its time, was nonetheless simple and robust. The ACMA is hopeful that as this code is internalised and operationalised by industry, co-regulation can contribute effectively to making the networked world of the future 'work' as effectively and as simply as the telegraph for the benefit of all parties; consumers, citizens, industry and government. It is in large part directed at empowering members of our networked society to protect their own interests – arming them with the information they need to get the responses they need from whoever their provider may be – as well as requiring service providers to put in place the structures necessary to provide what their customers will now be empowered to demand.

More significantly, the code is intended to bring about a cultural shift in the way providers go about customer care. It's now up to industry to prove its mettle. The ACMA for its part will be stepping up the compliance and enforcement work necessary to make the TCP Code work (that is, really work) in the interests of consumers and establish a new balance in the way the industry deals with its customers. I am hopeful that most players have bought into the necessity to lift their game both individually and collectively – we are, and will be, watching.

It is also my view that our close attention will be needed anyway – the digital economy marketplace is being turbo-charged (as I've repeatedly highlighted today); and as I've also highlighted, it is increasingly fast and transaction dense, operating in terms of value networks rather than value chains, with embedded international links and nodes.

And again, my overriding proposition – what is, and will be needed, is regulation that is 'fit for purpose', intervention that is enough to do the job in a specific circumstance, and no more. This means regulation that is evidence-informed and that engages all stakeholders; industry, consumers, citizens, legislators, and ourselves as regulators.

## what is needed, is regulation that is 'fit for purpose', intervention that is enough to do the job in a specific circumstance, and no more

The current, let alone emerging, communications and media environment does not allow a simple singular answer to how we should be regulating communications and media today – let alone in the hyper-connected, networked society world of tomorrow. The environment is too multi-dimensional, too heavily textured for that.

And thank you again for the honour of presenting this year's Charles Todd Oration, which I've interpreted as a compliment to the consistently fine work that the ACMA has been delivering over the last several years. I hope my remarks have given you some cause for reflection.

***This is an abridged version of the speech delivered by Chris Chapman at the Charles Todd Oration on 30 August 2012. An expanded version can be located on the ACMA website at http://www.acma.gov.au/webwr/_assets/main/lib410189/chris_chapman_speech-charles_todd_oration.pdf***

# Towards an Australian Law of Privacy: The Arguments For and Against[1]

**David Rolph examines the arguments for and against a statutory cause of action for serious invasion of privacy.**

## Introduction

The issue of how best to protect privacy has recently been a matter of intense interest to Australian law reform commissions. Within the last five years, three law reform commissions have produced reports on the issue,[2] all of which have recommended the introduction of a statutory cause of action in some form.[3] In response to part of the three volume Australian Law Reform Commission's report, *For Your Information: Australian Law and Practice*, the then responsible Minister,[4] the Minister for Privacy and Freedom of Information, the Hon. Brendan O'Connor, released an issues paper on 'a Commonwealth statutory cause of action for serious invasion of privacy' (the ***Issues Paper***).[5] As part of the consultation process, the Minister received submissions from a wide range of individuals and organisations, including bar associations, law societies, media organisations, peak industry bodies, community legal centres and academics. This consultation process represents the most recent development in privacy law reform in Australia, which may or may not result in the introduction of a statutory cause of action for serious invasion of privacy.

The purpose of this article is to analyse the submissions made as part of the consultation process.[6] Given the number and variety of the arguments made in the submissions, it is not possible to analyse them exhaustively. This paper focuses on the most common and the most interesting arguments made for and against a statutory cause of action for serious invasion of privacy. The submissions provide useful insights into the state of the privacy debate in Australia, particularly the issues of whether there needs to be a cause of action for invasion of privacy recognised or introduced and, if so, what form it should take. They reveal that there is real division as to the need and the desirability of having some form of direct, comprehensive right to privacy in Australian law. Consequently, there is real doubt as to whether this proposal will be enacted and, if enacted, how effective it will be.

## The Issues Paper

The *Issues Paper* is organised around a list of nineteen questions.[7] The threshold issue identified by the *Issues Paper* is whether a statutory cause of action for invasion of privacy is necessary. The Minister, in his foreword, makes it clear that the impetus for considering whether such a cause of action should be introduced is the intrusive potential of recent technological developments.[8] Characterising the place of privacy in contemporary Australian society, the *Issues Paper* observes that 'the privacy context is drastically different from that of 1937, and indeed the whole of the 20th century'.[9] In order to demonstrate the extent of the technological changes, the *Issues Paper* documents the levels of household access to computers; the rates of mobile phone ownership;[10] the extent of wired and wireless internet connection and usage;[11] and the rise of social media.[12] The *Issues Paper* then does the following:

- seeks views on whether 'recent developments in technology mean that additional ways of protecting individuals' privacy should be considered in Australia';[13]
- canvasses the treatment of privacy under Australian, United States, European Union, United Kingdom, Canadian and New Zealand law;[14]
- identifies the related threshold issue as being whether, outside the concerns about intrusive technologies, there are additional reasons for or against the introduction of a statutory cause of action for invasion of privacy;[15]
- canvasses arguments in favour of such a cause of action, including the inadequacy of existing privacy protections under Australian law; the need for comprehensive, rather than piecemeal, privacy protection; the need to 'fill the gaps'; the desire to create, in the words of Professor John Burrows, 'a climate of

---

1 This article is an edited version of a paper given at the 'Comparative Perspectives on Privacy and Media Law Conference' at the University of Cambridge in June 2012.

2 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) ('ALRC'); New South Wales Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) ('NSWLRC'); Victorian Law Reform Commission, *Surveillance in Public Places*, Final Report No 18 (2010) ('VLRC').

3 ALRC, Recommendation 74-1; NSWLRC, Recommendation; VLRC, Recommendations 22-24. For an analysis of these three law reform proposals, see Normann Witzleb, 'A Statutory Cause of Action for Privacy? A Critical Appraisal of Three Recent Australian Law Reform Proposals' (2011) 19 *Torts Law Journal* 104.

4 Following a Cabinet reshuffle in mid-December 2011, responsibility for privacy law reform was assigned to the Attorney-General, the Hon. Nicola Roxon.

5 Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Issues Paper: A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy*, September 2011: http://www.dpmc.gov.au/privacy/causeofaction/ ('*Issues Paper*').

6 The submissions made in response to the *Issues Paper* can be found at http://www.ag.gov.au/Consultationsreformsandreviews/Pages/ACommonwealthStatutoryCauseofActionforSeriousInvasionofPrivacy.aspx

7 For the full list of questions, see *Issues Paper*, pp. 52-53.

8 *Issues Paper*, p. 3.

9 *Issues Paper*, p. 9.

10 *Issues Paper*, p. 9.

11 *Issues Paper*, p. 10.

12 *Issues Paper*, p. 11.

13 *Issues Paper*, Question 1.

14 *Issues Paper*, pp. 13-22.

15 *Issues Paper*, Question 2.

restraint', so as to prevent invasions of privacy from occurring in the first place (akin to a 'chilling effect'); and the need to give effect to Australia's human rights obligations;[16]

- canvasses arguments tending against the introduction of such a cause of action, including the notorious difficulty of defining privacy; the potential adverse impact on commercial activities, law enforcement and national security; and concerns about freedom of expression, freedom of the press and artistic freedom;[17]

**there is real division as to the need and the desirability of having some form of direct, comprehensive right to privacy in Australian law**

- considers whether a cause of action for invasion of privacy (if it were to be developed) ought to be created under statute or left to the courts to develop the common law.[18] In its consideration, the *Issues Paper* notes that if the cause of action were to be statutory, there is the additional issue of whether it should be enacted by the Commonwealth Parliament or by the States and Territories.[19] A federal statute would ensure that there was consistent, national legislation but there are constitutional constraints on the power of the Commonwealth Parliament to legislate for such a cause of action. The Commonwealth could attempt to have the States and Territories refer their legislative power to it but there is no guarantee that any or all of them would do so. If all of the States and Territories did not refer their legislative power to the Commonwealth, there would be legislative diversity, which would be an undesirable outcome. By contrast, there are no such constitutional limitations on the States and Territories to legislate such a cause of action but, without a coordinate scheme, there might end up being legislative diversity in any event. Even with such a coordinate scheme, a State or a Territory could elect to amend its own law, again creating legislative diversity;
- addresses the elements of a potential statutory cause of action for serious invasion of privacy, including the central questions as to whether the standard of liability should be one of 'highly offensive to a reasonable person of ordinary sensibilities';[20] whether the public interest should be balanced against privacy at the level of liability or whether it should constitute a free-standing defence;[21] whether the fault element should be limited to intent and recklessness or whether it should extend to negligence;[22] and whether the legislation should include a range of factors or a non-exhaustive list of activities to illustrate when liability might or might not be established;[23] and
- seeks views about what defences should be available;[24] whether certain organisations should be excluded from the operation of the cause of action;[25] what remedies should be available and, more particularly, whether a cap should be imposed on damages for non-economic loss;[26] whether the cause of action should be actionable without proof of damage;[27] whether there should be an offer of amends process;[28] whether the cause of action should be restricted to natural persons;[29] whether the cause of action should be restricted to living persons;[30] the appropriate limitation period for such claims;[31] and the proper forum in which such claims should be determined.[32]

## The Arguments in Favour of a Statutory Cause of Action for Serious Invasion of Privacy

Given the constraints of space and the complexity of the issues raised by the *Issues Paper*, it is not possible to analyse in detail all of the arguments for and against a statutory cause of action for serious invasion of privacy. In looking at the submissions made as part of the consultation process, there are some common themes which emerge.

The most prominent and interrelated arguments in support of a statutory cause of action for invasion of privacy were that the existing legal protections under Australian law were inadequate and that technological changes necessitated such a legislative change. The submissions varied in the extent to which they took these matters to be self-evident. For example, in its submission, the firm of plaintiff lawyers, Maurice Blackburn, argued that it was important for Australian law to keep pace with technological changes and that there was a role for government in improving the protection of individual privacy.[33] It noted that there were instances in which an individual could have his or her privacy invaded but be left without adequate legal redress.

A similar point was made in the submission of the Queensland Office of the Information Commissioner ('the *QOIC*'), which pointed out that the privacy legislation in Queensland was directed to protect information privacy and imposed obligations on government agencies in relation to the collection, storage, usage and disclosure

16 *Issues Paper*, pp. 23-26.

17 *Issues Paper*, pp. 26-28.

18 *Issues Paper*, Question 3.

19 *Issues Paper*, p. 29.

20 *Issues Paper*, Question 4.

21 *Issues Paper*, Questions 5 and 6.

22 *Issues Paper*, Question 7.

23 *Issues Paper*, Questions 8 and 9.

24 *Issues Paper*, Question 10.

25 *Issues Paper*, Question 11.

26 *Issues Paper*, Questions 12 and 13.

27 *Issues Paper*, Question 14.

28 *Issues Paper*, Question 15.

29 *Issues Paper*, Question 16.

30 *Issues Paper*, Question 17.

31 *Issues Paper*, Question 18.

32 *Issues Paper*, Question 19.

33 For other examples of submissions citing the inadequacy of existing legal protections in Australia and the challenges to privacy posed by technological developments, see the submissions by the New South Wales Council for Civil Liberties, the Australian Privacy Foundation, the National Welfare Rights Network, the Queensland Council for Civil Liberties, Liberty Victoria, the Public Interest Advocacy Centre and the Office of the Victorian Privacy Commissioner.

of such information.[34] The QOIC noted that a person whose privacy was invaded by an individual, a small business or a community organisation, for example, would not have a similar right of legal redress. This highlights one of the major issues identified in the law reform process, namely whether the purpose of a statutory cause of action for invasion of privacy is to fill the gaps left by Australian law's existing protection of privacy or whether it is to provide a new, free-standing, comprehensive cause of action which will operate alongside and in addition to existing causes of action available to plaintiffs. If the purpose is to fill the gaps, then those gaps have to be identified and the legislative solutions need to be tailored to those gaps.

Amongst those supporting the introduction of a cause of action for invasion of privacy, there were, in certain submissions, a strong preference for the legislature to intervene, rather than leaving the common law to be developed by the courts.[35] This was informed by an observation of the relative non-development of the common law in the decade after the High Court's decision in *ABC v Lenah Game Meats*.[36] Perhaps the most developed arguments in favour of the legislature rather than the common law was provided by the Public Interest Advocacy Centre (***PIAC***). It expressed the view that '[a]s a general principle, significant law reform should occur via the legislature'. PIAC then identified the benefits of a statutory cause of action: it provided greater certainty, clarity and predictability about rights, responsibilities and liabilities; the legislature was better placed than the courts to take into account the full range of countervailing rights and interests; the legislature was also better placed than the courts to be more flexible about remedies; and if the development of the law in this regard were left to the courts, there was no guarantee that reform would happen at all.

The benefits of the legislature, rather than the courts, developing a cause of action for invasion of privacy should not be overstated. For instance, even though all of the Australian law reform proposals recommend a statutory cause of action, the terms of the proposals are all so open-textured – understandably, given the diffuse nature of privacy as a concept – that the application of any of these proposals to concrete facts would require considerable judicial interpretation. This ultimate dependence upon judicial interpretation might lessen the certainty, clarity and predictability claimed for a statutory cause of action, for example. Nevertheless, this tension between the preference for a statutory or a common law development of a right to privacy highlights the centrality of questions of legal method in the privacy law reform debate.

A number of submissions supported the introduction of a statutory cause of action for serious invasion of privacy on the basis that it would implement Australia's obligations under the *International Covenant on Civil and Political Rights* ('*ICCPR*').[37] Australia is a signatory to the ICCPR but, to the extent that it has been enacted in domestic law under the *Privacy Act 1988* (Cth), does not provide a remedy for all forms of invasion of privacy, being directed instead to the protection of information privacy. Under Art 17, individuals have a right to be protected against 'unlawful and arbitrary interference with his (or her) privacy' and under Art 2(3), individuals are entitled to an 'effective remedy' in respect of such an interference.

**whether the purpose of a statutory cause of action for invasion of privacy is to fill the gaps left by Australian law's existing protection of privacy or whether it is to provide a new, free-standing, comprehensive cause of action which will operate alongside and in addition to existing causes of action available to plaintiffs**

In Australia, arguments based on human rights are unlikely to be given weight by legislators. Australia has no constitutional or statutory protection of human rights at a national level. In December 2008, under the former Labor Prime Minister, Kevin Rudd, a panel of eminent Australians were commissioned to conduct a consultation on the protection of human rights in Australia.[38] The National Human Rights Consultation Committee (the ***NHRCC***) reported to the then Attorney-General, the Hon. Robert McClelland, in late September 2009,[39] recommending the introduction of a Federal Human Rights Act.[40] In its terms, the report recognised that there already existed significant political opposition to such a development in Australia, thus made additional recommendations on the basis that comprehensive human rights legislation would not be introduced. The NHRCC was correct – opposition to the introduction of a Federal Human Rights Act from both major parties led to lesser measures being introduced, the most notable being the passage of the *Human Rights (Parliamentary Scrutiny) Act 2011* (Cth), which created the Parliamentary Joint Committee on Human Rights, with oversight of the compatibility of Commonwealth legislation with human rights, and the requirement that bills and certain legislative instruments be accompanied by a statement of compatibility, which statement is not binding on any court or tribunal and the absence of which did not affect their validity.[41]

At a State and Territory level, only the Australian Capital Territory and Victoria have comprehensive human rights legislation.[42] One of the enumerated rights protected is the right to privacy.[43] It is telling that, in both jurisdictions, notwithstanding the fact that human rights legislation has been in place for several years, the presence of a right to privacy has not been the stimulus for any development of the common law. There appears to have been no judicial consideration of the right to privacy. The status of the human rights legisla-

34 The relevant legislation is the *Information Privacy Act 2009* (Qld).

35 See, for example, the submissions of Maurice Blackburn Lawyers, the Office of the Australian Information Commissioner, Liberty Victoria and the Office of the Victorian Privacy Commissioner.

36 See, for example, the submissions of Maurice Blackburn Lawyers, Liberty Victoria, the New South Wales Council of Civil Liberties and the Office of the Victorian Privacy Commissioner.

37 See, for example, the submissions of the Office of the Australian Information Commissioner; Maurice Blackburn Lawyers; Liberty Victoria; and New South Wales Law Society Human Rights Committee. See also the submission of the Queensland Council for Civil Liberties and the Australian Athletes' Alliance (implementation of Australia's obligations under the *Universal Declaration of Human Rights*).

38 As to the panel members, see http://www.humanrightsconsultation.gov.au/Who/Pages/default.aspx.

39 The full report of the NHRCC can be found at http://www.humanrightsconsultation.gov.au/Report/Pages/default.aspx.

40 NHRCC, Recommendation 18.

41 As to the Federal Government's response to the NHRCC, see http://www.ag.gov.au/Humanrightsandantidiscrimination/Australiashumanrightsframework/Pages/default.aspx.

42 *Human Rights Act 2004* (ACT); *Charter of Human Rights and Responsibilities Act 2006* (Vic).

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

tion in Victoria is somewhat precarious. In April 2011, the newly elected Victorian State Government, under Liberal Premier, Ted Baillieu, commissioned a review of the Victorian *Charter of Rights and Responsibilities Act 2006*.[44] The report recommended the winding back of the legislation in important respects,[45] although not all of the recommendations were accepted by the Baillieu Government,[46] notwithstanding the fact that it had the majority of members on the review committee. There are no present, concrete plans to introduce human rights in any other Australian jurisdiction.[47]

Given the absence of direct, comprehensive human rights protections in Australia and the bipartisan political aversion to such protections, arguments in favour of a statutory cause of action for serious invasion of privacy based on human rights are unlikely to contribute significantly to any impetus for this proposed reform.

**this tension between the preference for a statutory or a common law development of a right to privacy highlights the centrality of questions of legal method in the privacy law reform debate**

### The Arguments against a Statutory Cause of Action for Serious Invasion of Privacy

Whilst one of the central arguments in favour of a statutory cause of action for invasion of privacy was that the existing protections of privacy under Australian law were inadequate, those opposed to the proposed reform took a different view on this issue. For example, the Special Broadcasting Service (***SBS***), Australia's national public multicultural broadcaster, submitted that there were already substantial protections of privacy under Commonwealth, State and Territory laws, as well as at common law and in equity. Therefore, in SBS' view, there was no need for an additional cause of action for invasion of privacy.[48] Obviously, whether the existing protections of privacy under Australian law were adequate or inadequate is a matter about which different views might be expressed. However, SBS' submission indirectly suggests that there might be another useful way of analysing this issue, namely by asking whether the existing protections of privacy, as fragmentary and as overlapping as they are, are rational.

A related argument advanced by submissions opposing the introduction of a statutory cause of action for invasion of privacy was that the need for such a reform has not been demonstrated.[49] For instance, SBS and Free TV Australia, in their separate submissions, pointed out that there were few complaints received about invasion of privacy, from which they concluded that there was no substantial evidence to suggest that media intrusion upon personal privacy was a major issue in Australia. The Rule of Law Institute inferred from the lack of cases brought before Australian courts directed to developing the common law of privacy after the High Court's decision in *ABC v Lenah Game Meats* that there was little demand for such a cause of action.[50] It went further, asserting that, to the extent that the impetus for the proposed reform was the *News of the World* phone hacking scandal, there was no evidence that Rupert Murdoch's Australian media outlets engaged in such practices.[51]

The inferences drawn in the submissions are problematic. The failure by individuals to complain about intrusions upon privacy, let alone to litigate them, does not necessarily mean that no intrusions in fact occurred. There are a range of plausible reasons why people who feel that their privacy has been invaded by the media might not complain or sue. People might not complain to a media outlet because, for example:

- they do not feel that their complaint will be taken seriously and thus it will be a waste of their time and effort or that the outcome will not be satisfactory; people might not sue because litigation is expensive;
- the claim, if it is unable to be accommodated within an existing cause of action, is speculative, thereby heightening the inherent uncertainty of litigation; and/or
- litigation would give publicity to the intrusion upon privacy, thereby reinforcing the hurt and humiliation inflicted by the initial intrusion.

This is not an exhaustive list but rather demonstrates that the inferences drawn in these submissions about the level of concern about media intrusion upon personal privacy are not the only available ones.[52] The other observation that can be made about these submissions is that they are underpinned by an implicit understanding that law reform is most justifiable when there is an empirically demonstrated need. Establishing or quantifying the extent of public concern about intrusive media practices might be a difficult task. Even if it were possible, it does not provide the only basis for law reform. Even if a need for this law reform cannot be empirically demonstrated, it might be justifiable on the basis of principle or rationality.

The strongest and most obvious argument against a statutory cause of action for serious invasion of privacy was a concern about the impact of the proposed law reform on freedom of expression and freedom of the press.[53] The concern is understandable, given the absence of any comprehensive constitutional or statutory protection of freedom of expression. Speech in relation to government or political matters may attract the protection of the implied freedom of

---

44 Under the *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 44, the Attorney-General was required to conduct a review of the first four years of operation of the legislation. As to the terms of reference of the review, see http://www.parliament.vic.gov.au/sarc/article/1448. Under the *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 45, a further review of the fifth to eighth years of operation of the legislation is also required.

45 As to the report of the review committee, see http://www.parliament.vic.gov.au/sarc/article/1446.

46 As to the government response to the recommendations made in the report of the review committee, see http://www.parliament.vic.gov.au/sarc/article/1446.

47 A consultation process on the introduction of a *Charter of Human Rights and Responsibilities* in Tasmania appears not to have resulted in the presentation of a bill to the Tasmanian Parliament. As to the consultation process and the submissions received, see http://www.justice.tas.gov.au/corporateinfo/projects/human_rights_charter.

48 See also the submission of the Australian Subscription Television & Radio Association, the Arts Law Centre of Australia and the Australian Direct Marketing Association.

49 See, for example, the submissions of Free TV Australia, the Rule of Law Institute, S.B.S., the Australian Subscription Television & Radio Association, Commercial Radio Australia, the Australian Bankers' Association and News Ltd.

50 See also the submission of News Ltd. As to the lack of public demand for further privacy protections more generally, see the submission of S.B.S., Free TV Australia, the Australian Direct Marketing Association and Optus.

51 See also the submissions of Free TV Australia and the Australian Bankers' Association.

52 See also the submission of the Law Institute of Victoria.

53 See, for example, the submissions of Free TV Australia, News Ltd, the Rule of Law Institute, S.B.S. and Telstra.

political communication but, beyond that, freedom of expression is a value underlying Australian law which is not directly protected; it is a freedom which often yields to countervailing rights and interests, which is evidenced by the largely unhappy experience of defendants in defamation proceedings in Australia. A concern about augmenting plaintiffs' rights, particularly in relation to the protection of dignitary interests, is understandable without effective guarantees of freedom of expression and freedom of the press.

The potential 'chilling effect' of a statutory cause of action for invasion of privacy on certain forms of expression was noted by some submissions. For example, Transparency International Australia noted that the exposure of corruption could be made more difficult by a general, enforceable right to privacy and urged caution in the formulation of any such cause of action. The Arts Law Centre of Australia was particularly concerned about the 'chilling effect' of a statutory cause of action for invasion of privacy on artistic expression. It maintained that such a cause of action should not be introduced without a strong human rights framework also being introduced. Crucial to a human rights framework would be express protection of freedom of expression.

The concern about the potential negative impact of a statutory right to privacy on freedom of expression and freedom of the press was not limited to those individuals and bodies which opposed such a right. For example, the trade union, the Media, Entertainment and Arts Alliance (the ***MEAA***) expressed no firm view on whether a statutory cause of action for invasion of privacy should be introduced but was emphatic that, if such a right were introduced, it should only occur if there were equal or stronger protections for freedom of expression introduced. The MEAA was concerned that freedom of expression is not adequately protected under Australian law and that any protection introduced as part of a statutory cause of action for invasion of privacy should be serious and substantial, not a 'mere passing reference'. The New South Wales Council for Civil Liberties (the ***NSWCCL***) strongly supported the introduction of a statutory cause of action for invasion of privacy but equally supported the introduction of a right to freedom of expression, including freedom of the press. In order to give it proper weight, the NSWCCL recognised that such a countervailing right be enshrined in its own separate legislation, rather than being protected incidentally as part of a statutory cause of action for invasion of privacy. Importantly, though, a number of submissions pointed out that undue weight should not be given to concerns about freedom of expression and freedom of the press, in the sense that a cause of action for invasion of privacy is not directed solely at media conduct.[54] Invasions of privacy by non-media actors might not raise issues of freedom of expression and freedom of the press.

The 'chilling effect' of the proposed reform was not only directed at freedom of expression and freedom of the press. A number of submissions identified the adverse impact on business. The common problems identified by the introduction of a statutory cause of action for invasion of privacy were:

- the creation of uncertainty;
- the encouragement of a litigious culture, particularly spurious claims;
- the increase in legal risk and compliance costs; the stifling of innovation, particularly technological developments; and
- generally making Australia more uncompetitive as a place to conduct business and to invest.[55]

A number of submissions strongly urged that a regulatory impact assessment be undertaken before this reform is introduced.[56] Given that a statutory cause of action for invasion of privacy will not be limited in its scope of operation to media conduct, there are legitimate concerns on the part of business as to how such a reform will cut across or undermine existing regulatory arrangements.

## Conclusion

Predicting how Australian privacy law reform might proceed is difficult. A case which has the potential to become a test case for whether the common law of Australia recognises an enforceable right to privacy is currently before the Supreme Court of New South Wales. At the time of writing, Hall J has reserved judgment on an application to strike out a claim by a former Commonwealth Bank employee, Victoria Saad, against the bank for infringement of such a right. Saad claims that images of her were misused by the Commonwealth Bank and the security firm it uses, Chubb Security Australia, on a fake Facebook page.[57] Whether the matter will survive the strike-out application and proceeds to final judgment remains to be seen.

**The potential 'chilling effect' of a statutory cause of action for invasion of privacy on certain forms of expression was noted by some submissions**

On the legislative front, the Federal Government has responded to the first part of the ALRC's recommendation about privacy law reform, which did not include the statutory cause of action for serious invasion of privacy.[58] The Government has not responded yet to the consultation process. It finds itself in a difficult political position, which might make it hard for it to legislate such a reform, particularly given the concerted opposition of a number of media outlets to a cause of action for invasion of privacy. Interestingly, however, the Federal Government Whip, Joel Fitzgibbon, used the Craig Thomson affair as a basis for renewing calls for the introduction of a statutory cause of action for privacy.[59] Whether this incident will provide the impetus for such a cause of action also remains to be seen.[60] The treatments of privacy before the courts and the legislature in Australia has reached the position where there is a lot of interest but seemingly little action.

***David Rolph is an Associate Professor at the Faculty of Law, University of Sydney, and an accomplished author, specialising in the areas of torts, media law, intellectual property, defamation and privacy. He also serves on the editorial board of various publications, including the Communications Law Bulletin.*** ***The author wishes to thank Joanna Connolly for her excellent research assistance. Any errors remain his own.***

54 See, for example, the Australian Broadcasting Corporation, the New South Wales Law Reform Commission and the Australian Privacy Foundation.

55 See, for example, the submissions of Free TV Australia, Telstra, Commercial Radio Australia, the Australian Association of National Advertisers, the Australian Direct Marketing Association and the Australian Bankers' Association.

56 See, for example, the submissions of the Australian Direct Marketing Association, Optus and the Research Industry Council of Australia.

57 See http://www.glj.com.au/1703-article (password required).

58 Gemma Daley and Mark Skulley, 'Fitzgibbon lashes media over Craig Thomson affair', The Australian Financial Review, 7 June 2012; Nick Leys, 'New privacy laws still long way off, despite whip's call', The Australian, 8 June 2012.

59 Gemma Daley and Mark Skulley, 'Fitzgibbon lashes media over Craig Thomson affair', *The Australian Financial Review*, 7 June 2012.

60 Nick Leys, 'New privacy laws still long way off, despite whip's call', *The Australian*, 8 June 2012.

# Appendix

Submissions in favour of a statutory cause of action for serious invasion of privacy include:

- National Welfare Rights Network
- Queensland Office of the Information Commissioner
- Office of the Australian Information Commissioner
- Maurice Blackburn Lawyers
- New South Council for Civil Liberties
- Australian Privacy Foundation
- Queensland Council for Civil Liberties
- Federation of Community Legal Centres
- New South Wales Law Reform Commission
- Australian Athletes' Alliance
- Privacy Committee of South Australia
- Law Institute of Victoria
- Public Interest Advocacy Centre
- Office of the New South Wales Privacy Commissioner
- Office of the Victorian Privacy Commissioner
- Human Rights Committee of the Law Society of New South Wales
- Castan Centre for Human Rights Law

Submissions opposed to a statutory cause of action for serious invasion of privacy include:

- Fundraising Institute Australia
- S.B.S.
- Free TV Australia
- Australian Subscription Television & Radio Association
- Arts Law Centre of Australia
- Commercial Radio Australia
- Telstra
- Australian Association of National Advertisers
- Australian Direct Marketing Association
- Optus
- Australian Bankers' Association
- News Ltd
- Rule of Law Institute

Submissions expressing no firm view on a statutory cause of action for serious invasion of privacy and / or dedicated to a specific issue or industry include:

- Mental Health Law Centre (WA) Inc.
- Transparency International Australia
- Insurance Council of Australia
- Mindframe National Media Initiative
- Australian Broadcasting Corporation
- Law Council of Australia
- Australian Finance Conference
- Research Industry Council of Australia
- SupportLink
- Media, Entertainment and Arts Alliance

# ALRC Inquiry - Copyright and the Digital Economy

**Rebecca Sadleir and Hamish Collings-Begg consider the recently released Australian Law Reform Commission issues paper on the use of copyright in the digital economy.**

## Background to the Inquiry

On 20 August 2012, the Australian Law Reform Commission (the ***ALRC***) released an issues paper as part of its inquiry into the use of copyright in the digital economy.[1] The inquiry recognises that Australian copyright laws are no longer adequate in light of the rapidly developing technological environment in which they operate, and seeks public submissions on possible reforms.

The relevance of this inquiry to the general public is exemplified by the high-profile *Optus TV Now* case.[2] On 7 September 2012, the High Court refused Optus' application for special leave to appeal, and Optus has now publicly stated that it will turn to this inquiry in the hope of reform to the law. Optus' vice-president of corporate and regulatory affairs, David Epstein, has said:

> Our service is a high-profile example of the kind of breakthroughs that can be delivered using the latest mobile, computing and cloud technologies … It's essential we encourage and support innovation and investment in these new markets. If we don't, we'll end up buying services from overseas rather than building a domestic digital economy.[3]

## Overview

The issues paper defines the digital economy as 'the global network of economic and social activities that are enabled by information and communications technologies, such as the internet, mobile, and sensor networks', and recognises that the Australian economy is moving towards a greater reliance on high-efficiency, knowledge-intensive industries.

The issues paper calls for public submissions on over 50 questions, covering 16 broad areas identified by the ALRC. For each of these areas, the paper considers options to achieve greater availability of copyright material in ways that are socially and economically beneficial. The paper considers in detail the possibility of a generalised 'fair use' exception to replace many specific areas which are currently covered by an exception, whilst seeking to remain flexible to the possibility of new areas that require exceptions to copyright infringement.

The scope of the inquiry is limited to considering exceptions to copyright and statutory licensing schemes, and does not cover more radical options, such as an 'opt-in' or 'opt-out' regime for copyright protection.

## Guiding principles for reform

The paper sets out eight key principles, according to which the reforms should:

(a) promote the development of a digital economy by providing incentives for innovation in technologies and access to content;

(b) encourage innovation and competition and not disadvantage Australian content creators, service providers or users;

(c) recognise the interests of rights holders and be consistent with Australia's international treaty obligations, including the *Berne Convention*;[4]

(d) promote fair access to and wide dissemination of content;

(e) ensure copyright law is able to respond adequately to technological change;

(f) acknowledge the 'real world' ways that copyright materials are used;

(g) promote clarity and certainty for creators, rights holders and users; and

(h) promote an adaptive, efficient and flexible framework.

The following is an overview of the 16 key areas identified by the issues paper.

## Australian copyright laws are no longer adequate in light of the rapidly developing technological environment in which they operate

## Caching, indexing and other internet functions

The paper considers the processes of caching, indexing and similar technical functions, which are essential to the efficient operation of the internet.

It is currently unclear whether caching and indexing infringe copyright. The processes can involve the copying of works and communicating them to the public, for example when a search engine displays its results. There are several current exceptions which may arguably apply - the exceptions allowing temporary reproduction of material as part of a 'technical process of making or receiving communication';[5] reproduction of material on the system of a carriage service provider in response to an action by a user, to facilitate efficient access to that material;[6] and automated caching by an educational institutional for certain purposes[7] - but these exceptions may not adequately cover caching and indexing.

The ALRC suggests that reform of this area of the law may include clarifying or broadening the current exceptions, creating a new specific exception, or creating a broad and flexible exception to permit these processes. The paper notes how other jurisdictions, such as the UK and Canada, have specific exceptions allowing caching, whereas the US allows caching under a fair use doctrine.

---

1 The Australian Law Reform Commission, *Copyright and the Digital Economy,* Issues Paper (2012) is available at http://www.alrc.gov.au/publications/copyright-ip42.

2 *National Rugby League Investments Pty Ltd v Singtel Optus* (2012) 201 FCR 147.

3 David Epstein, 'The law left behind by technology' (10 September 2012) *Australian Financial Review*, http://afr.com/p/opinion/the_law_left_behind_by_technology_ayRHLRzGN8zRugjYDNgqEJ (accessed 10 September 2012).

4 *Berne Convention for the Protection of Literary and Artistic Works (Paris Act)*, 24 July 1971, [1978] ATS 5 (entered into force on 15 December 1972).

5 *Copyright Act 1968* (Cth) ss 43A, 111A.

6 Ibid, ss 116AB, 116AG.

7 Ibid, s 200AAA.

## Cloud computing

The issues paper highlights the increasing use of cloud computing services for storage and content delivery, and recognises that cloud computing represents a major development in the digital environment. Use of cloud computing services can facilitate copyright infringement, for example where illegally-obtained content is uploaded to the cloud, or where content is copied to the cloud for download to multiple devices (a key issue in the *Optus TV Now* case). This is not only an issue for end users, and the paper highlights the risks that companies offering cloud computing services are exposed to under the current law.

The issues paper seeks views on whether current copyright law is impeding cloud computing services, and whether exceptions in the *Copyright Act* should be amended or introduced to account for this technology.

**cloud computing represents a major development in the digital environment. Use of cloud computing services can facilitate copyright infringement**

## Copying for private use

The paper considers the three exceptions which allow copying for private use, and seeks public comment on whether they should be clarified or expanded.

(a) First, the *format-shifting* exception, which allows users to make copies of copyright material into other specified formats.[8] The paper notes in particular that this may not apply to cloud computing services, nor to the digital-to-digital copying of films.

(b) Secondly, the *time-shifting* exception, which allows users to make copies of certain materials to watch at a more convenient time.[9] The issues paper notes the importance of the time-shifting exception in relation to cloud computing, and content made available using the internet or internet protocol television (IPTV).

The ALRC stresses the importance of wording this exception so as not to exclude future technological developments. It also notes that the issue which arose in the *Optus TV Now* case – that is, whether the time shifting exception applies to copying by a company on behalf of an individual – should be considered in the reforms. In this context, the issues paper considers whether a simplified exception for reproductions for private purposes is needed, or alternatively whether a broad and flexible 'fair' or 'reasonable' use exception is preferable.

(c) Thirdly, the paper considers the exception allowing the copying and storage of copyright material for the purpose of back-up and data recovery.[10] Again, this is highly relevant in the cloud computing context.

## Online use for social, private or domestic purposes

The paper notes the widespread use of copyright materials for social, private and domestic purposes, specifically the uploading and sharing of non-commercial user-generated content on social networking and other sites. User-generated content may include the use of excerpts from copyright materials, such as movies or music, in combination with 'a certain amount of creative effort' from the individual, for example, the adding of a commentary to the work. The paper notes that existing fair dealing exceptions may apply to user-generated content, such as for the purposes of criticism or review, or parody or satire.[11]

The issues paper considers whether a new specific exception should be introduced, allowing user-generated content that does not unjustifiably harm copyright owners, or whether a broader fair use doctrine would be more appropriate.

## Transformative use

The issues paper distinguishes 'transformative works' from user-generated content, on the basis that transformative works transform pre-existing works to create something new. Common forms of transformative works are 'sampling', 'remixes' and 'mashups', all of which may be made in commercial and non-commercial contexts.

These types of works may only in some cases be covered by the fair dealing exceptions. They may also infringe an author's moral rights.[12]

The paper considers a number of options for reform, such as an exception for non-commercial, transformative uses - as has been introduced recently in Canada - or a broader flexible exception for 'fair' or 'reasonable' use.

## Libraries, archives and digitisation

Many cultural institutions are undertaking a process of converting works they hold into a digital format, for the purposes of better preservation and wider dissemination. Digitisation may constitute copyright infringement, as it involves the reproduction, and often communication, of copyright material. The cost of obtaining the requisite licences constitutes a barrier to digitisation for libraries and archives.

The ALRC asks whether the *Copyright Act* should be changed to permit a wider range of digitisation practices by libraries and archives, whether a specific exception is required and, if so, whether it should be limited to non-commercial use that does not interfere with the copyright owner's market. The ALRC also considers whether a broad and flexible 'fair' or 'reasonable' use exception would be more appropriate in the context.

## Orphan works

Orphan works are works of which the author or owner cannot be found by a person wishing to make use of the work. The paper considers several models for orphan works, and seeks comment on which is most appropriate.

(a) First, a 'centrally granted licence' scheme, which allows a user to obtain a non-exclusive licence to use an orphan work, after reasonable efforts have been made to locate the owner. A royalty fee is paid to a central administrative body. This model is currently in use in Canada.

(b) Secondly, limitations on the monetary and injunctive relief available to an owner, where the user of an orphan work has conducted a reasonably diligent search.

(c) Thirdly, an extended collective licensing scheme where users pay licence fees to a statute-appointed body, which is authorised to grant licences for specific purposes on behalf of copyright owners.

(d) Finally and more generally, a non-commercial use exception for use of unpublished orphan works.

## Data and text mining

Data and text mining involves copying and analysing electronic information. The paper notes the growing value and usage of these tech-

8 Ibid, ss 43C, 47J, 110AA, 109A.

9 Ibid, s 111.

10 Ibid, s 47C.

11 *Copyright Act 1968* (Cth) ss 41, 103A; and 41A, 103AA respectively.

12 As was recently considered in *Perez v Fernandez* (2012) 260 FLR 1.

niques in Australia. Currently, these processes may constitute copyright infringement, unless they are covered by a fair dealing exception, which is often not the case. The paper considers whether a specific data mining exception should be created and, if so, whether it should be confined to non-commercial research.

## Educational institutions

There are currently two statutory licensing schemes which provide for the use of copyright material by educational institutions.[13] These schemes have been criticised, as fees are now collected for uses of otherwise free and publicly available material on the internet. Section 200AB of the *Copyright Act* provides an exception to infringement for the purpose of giving educational instruction and not for a profit, but this does not apply when one of the two schemes applies. The relationship between the schemes and the fair dealing exception for the purpose of research or study is unclear.

The ALRC seeks comment on how the exceptions could operate more effectively, and how the licensing schemes might be simplified.

## Crown use of copyright material

The ALRC seeks comment on whether the current Crown use regime in the Copyright Act is appropriate, and whether the scheme should apply to local government.

## Retransmission of free-to-air broadcasts

The copyright in free-to-air broadcasts are not infringed by retransmission of them, provided that remuneration is paid under the statutory licensing scheme.[14] This exception does not apply to retransmission which takes place over the internet.[15] The scheme provides for compensation of underlying rights holders, but not the free-to-air broadcasters.

The ALRC seeks comment on whether this exception should continue to operate, and whether it should be extended to broadcasts retransmitted over the internet.

## Statutory licences in the digital environment

The paper notes that improvements in the digital economy may offer opportunities to improve the operation of statutory licensing schemes. In particular, it notes how the internet can facilitate micro-licensing, by bridging the gap between rights holders and users. The ALRC seeks comment on whether the current licensing schemes are adequate and appropriate in the digital environment, or whether new schemes should be created.

## Fair dealing exceptions

The paper notes the current fair dealing exceptions to infringement, which allow for the use of materials for the purposes of research or study, criticism or review, parody or satire, reporting news, and for legal practitioners and patent and trade mark attorneys in giving professional advice.[16]

The paper considers whether these exceptions are adequate and appropriate in the digital environment. In particular, it considers simplification of the fair dealing exceptions, to create one fair dealing exception, which contain a non-exhaustive list of purposes, as well as a list of factors to be taken into account when considering if the dealing is 'fair'. The paper also considers whether there should be a specific fair dealing exception for the purposes of quotation.

## Other free-use exceptions

The paper makes the general comment that the current suite of statutory exceptions are unnecessarily complex. The ALRC seeks suggestions on how these exceptions might be simplified and better structured, to be more straightforward and comprehensible.

## Fair use

At multiple instances throughout the paper, the ALRC questions whether a more general 'fair use' exception would provide a more effective and appropriate system for exemption from infringement. The US copyright regime currently includes a fair use exception under which, to determine whether a use is 'fair', courts must consider:

(a) the purpose and character of the use;

(b) the nature of the copyrighted work;

(c) the amount and substantiality of the portion used; and

(d) the effect upon the market for the copyrighted work.

Arguments in favour of a fair use model are that it:

(a) enhances flexibility and timely responses to rapid technological changes;

(b) assists innovation; and

(c) can improve upon the utilisation of the current exceptions, which have been criticised as being too uncertain.

Arguments against an open-ended model are:

(a) the possible uncertainty of its application (although the paper notes that 'fair use' has proven to be a sufficiently certain term in the US);

(b) the need for litigation to determine its scope;

(c) the possibility of a 'chilling effect' in respect to the use of copyright material; and

(d) the lack of jurisprudence on the area in Australia.

The ALRC seeks comments, given the recent advances in technology, on whether a broad, flexible exception to copyright would now be possible and appropriate and, if so, how it should be framed.

**the paper highlights the risks that companies offering cloud computing services are exposed to under the current law**

## Contracting out

Finally, the paper considers and invites comment on whether copyright owners and users should be permitted to contract out of the operation of an exception.

## Process and Timing

Submissions on the 55 questions posed in the issues paper close on 16 November 2012. The ALRC is scheduled to release a discussion paper in mid-2013 including draft recommendations for reform. Following a further round of public consultation, the ALRC is due to deliver a final report to the Attorney-General by 30 November 2013.

***Rebecca Sadleir is a special counsel and Hamish Collings-Begg is a Law Graduate in the Intellectual Property Practice Group at Allens. The views expressed in this article are personal to the authors and do not represent any organisation.***

13 *Copyright Act 1968* (Cth) Pt VA, Pt VB.

14 Ibid, s 135ZZK.

15 Ibid, s 135ZZJA.

16 See *Copyright Act 1968* (Cth) ss 40(1), 103C(1); 41, 103A; 41A, 103AA; and 43(2) respectively.

# Interception Regulation up for Review

## Shane Barber & Lisa Vanderwal examine current proposals for telecommunications interception reform in light of changing technology and threats.

Australia's current telecommunications interception regime was established in 1979. In this pre-September 11 2001 environment, Australia and the world were simpler places in which to live. Many of the technological developments we take for granted today were simply unimaginable. Security threats too were a little more predictable.

In 2012 we are still served by the same core piece of legislation that served us in 1979, the *Telecommunications* (*Interception & Access*) Act 1979 (Cth) (***TIA***), albeit that it has been the subject of significant incremental change over the years. It is the powers afforded under the TIA which almost daily serve as a frontline tool used by law enforcement agencies in dealing with domestic and international security threats. It is also the TIA which, daily, seeks to balance the competing demands of protecting the rights of individuals to express themselves freely with the right of individuals to live free from the threats of others.

**It is the powers afforded under the TIA which almost daily serve as a frontline tool used by law enforcement agencies in dealing with domestic and international security threats**

In this article we briefly examine two recent developments in relation to the TIA. One represents yet the latest piece of tinkering with the TIA, in the form of the *Cybercrime Legislation Amendment Bill 2011* (the ***Bill***). The other reflects the opening salvo in a more comprehensive approach to telecommunications interception reform currently under consideration by the Parliamentary Joint Committee on Intelligence and Security (***Parliamentary Joint Committee***), using as the basis for its consideration a July 2012 discussion paper prepared by the Commonwealth Attorney General's Department entitled *Equipping Australia Against Emerging and Evolving Threats* (***Discussion Paper***).

### The Current Interception Regime

The TIA currently reflects a well-worn regime pursuant to which law enforcement agencies may require telecommunications carriers and carriage service providers (for the purpose of this paper, referred to as ***carriers***) to intercept and subsequently disclose communications passing over a network in real time, and also seek access to communications that have already passed over the network (known as stored communications).

The overriding principle of the TIA is that the privacy of users of telecommunications services in Australia is paramount, with the expectation being that any access to those communications by law enforcement agencies may only occur in tightly controlled circumstances. Generally, to access content, national security and law enforcement agencies must obtain an independently issued warrant and thereafter remain subject to a range of accountability measures. While exceptions are made in relation to, for instance, an employee of a carrier undertaking activities which are reasonably necessary to be done by that employee in order to perform certain duties effectively, even that exemption remains subject to court oversight.

Since it was assented to in October 1979, the TIA has been subject to no less than 78 pieces of amending legislation, not including the Bill. A key series of changes occurred in 2006 with the introduction of a chapter into the TIA dealing with stored communications. The drafters of the TIA could not have imagined back in 1979 many applications of communications networks taken for granted today which do not involve simple real time voice telephony. It is clear though that even with those significant 2006 changes dealing with evolving non-real time material, the legislation is failing to keep up with communications technology and the ingenuity of its users.

### The Parliamentary Enquiry

At the time of writing, the Parliamentary Joint Committee armed with terms of reference detailed in the Discussion Paper, has been conducting a series of meetings with stakeholders with a view to reporting to the Federal Government as to whether an entirely new interception regime, which better reflects the contemporary communications environment, should now be put into place.

The Discussion Paper reflects proposals for a package of changes in relation to national security, many of which go beyond recommendations for changes to the TIA. Other groups of proposals are:

- suggested amendments to the Telecommunications Act 1997 to:
  - establish a risk based regulatory framework to better manage national security challenges to Australia's telecommunications infrastructure;[1] and
- proposed reforms to the Australian Security Intelligence Organisation Act 1979 and the Intelligence Services Act 2001.

Insofar as the reforms directly relate to the TIA, in its terms of reference to the Parliamentary Joint Committee the Commonwealth Government has indicated that it wishes to progress the following proposals:

1. Strengthening the safeguards and privacy protection under the access regime in the TIA. This would include examination of:
   (a) the legislation's privacy protection objective;
   (b) the proportionality tests for issuing warrants;
   (c) mandatory record keeping standards; and
   (d) oversight arrangements by Commonwealth and State Ombudsmen.
2. Reforming lawful access to communications regime. This would include:
   (a) reducing the number of agencies eligible to access communication information;
   (b) the standardisation of warrant tests and thresholds;
   (c) streamlining and reducing complexity in the access regime. This would include:
      (i) simplifying the information sharing provisions that allow agencies to cooperate;
      (ii) removing legislative duplication; and
   (d) modernising the TIA's cost sharing framework to:
      (i) align industry interception assistance with industry regulatory policy; and

1 Equipping Australia Against Emergency and Evolving Threats, Attorney General's Department, July 2012, page. 4.

(ii) clarify the Australian Communications & Media Authority's regulatory enforcement role.

Stakeholders appear to agree that there is significant merit in those proposals.

While the Government has flagged its intention to now progress with those proposals, it has also asked the Parliamentary Joint Committee to consider a number of further measures including:

- creating a single warrant with multiple telecommunications interception powers; and
- expanding the number of telecommunications industry participants, beyond just carriers, to which the regulatory regime will apply.

In relation to the concept of a single category of warrant, industry experts have cautioned that such an approach does not take into account the fact that different thresholds are required for the exercise of different types of powers, which may need to be exercised by law enforcement and security authorities.[2]

> There are a range of difference activities with a range of different levels of intrusiveness … and they're reflected in the various levels of thresholds that apply to the granting of each of those warrants. What we're concerned about … is that in creating a single category of warrant we would be adopting a lowest common denominator approach.

The third item on the Government's wish list in relation to the TIA, and in relation to which it has asked the Parliamentary Joint Committee to report, includes matters such as establishing an offence for failure by industry participants to assist in the encryption of communications, to mandate industry response times and, most controversially, mandating data retention periods of up to two years for certain data. It is this latter proposal regarding data retention periods that has attracted significant attention due to the cost and inconvenience it will cause, the implications of which will ultimately be passed on to customers.

An example of how these reforms, if implemented, may manifest themselves in midsized carriers was provided in the submissions of iiNet to the Parliamentary Joint Committee in September 2012. In speaking to the Committee, iiNet's Chief Regulatory Officer, Steve Dalby, is reported as giving the following example:

> Dalby said that iiNet's total band width of 200Gbps could generate some 5 million URLs per second – data that, under the proposed legislation, the ISP would need to retain securely and reliably for two years. He said this would force the company to invest heavily in services and storage. 'We can currently purchase a 4TB disk for about $2,000 – we would need 10,000 of these to store 20,000TB of data. We'd put 10 of those in a rack so we would need 1000 racks' he said.
>
> Dolby added that iiNet would need to build a data centre to house the IT equipment, which would cost an estimated $30 million … All these costs, Dolby explained, would flow through to iiNet customers at an estimated $5 increase per month for all services.[3]

Similar sentiments are echoed by industry bodies such as Communications Alliance Limited and Australian Mobile Telecommunications Association (AMTA), which put forward a joint submission to the Parliamentary Joint Committee. The Australian Information Industry Association and the Australian Industry Group also endorsed the positions taken by Communications Alliance and AMTA in their submission. In their submission, the AMTA and Communications Alliance are reported to have suggested that the Federal Government has not provided sufficient justification for the proposed implementation of data retention and also cautioned that the policy approach to be adopted should see carriers in fact hold as little information as possible to avoid both loss of consumer privacy and any security threats to that information from unlawful access to the retained data itself.[4]

## The overriding principle of the TIA is that the privacy of users of telecommunications services in Australia is paramount, with the expectation being that any access to those communications by law enforcement agencies may only occur in tightly controlled circumstances

In the Discussion Paper, the Government makes its case for pushing this extensive reform by noting that:

- Lawful interception under the existing TIA arrangements is highly effective, taking into account the number of arrests, prosecutions and convictions based on lawfully intercepted material.
- Australia is and will remain a terrorist target for the foreseeable future, with jihadist terrorism being the most immediate threat. The Government cites at least four mass casualty attacks which have been disrupted in Australia in recent years due to the work of intelligence agencies. The Government points to the role of examining intercepted conversations in foiling some of these attacks.
- The rapid adoption of telecommunications technology and high speed broadband internet has expanded significantly the frequency of high tech crime being committed when compared to the environment that existed when the TIA was established in 1979. It argues that individuals involved in these activities are highly sophisticated, using highly effective software, ciphers, and other methodologies to impede detection by law enforcement agencies. Real time interception alone is increasingly underequipped to deal with these emerging threats.
- Duplication and complexity, which has arisen as a result of the large number of amendments made to the TIA over the years, needs to be removed.
- The number of telecommunications industry players has, of course, massively increased from the one significant player in 1979:

  > At the end of June 2011, there were 287 fixed line telephone service providers, three mobile network operators, 176 voice over internet protocol services providers, 33 satellite providers and 97 internet service providers (only including ISPs with at least 1,000 subscribers).[5]

- Australian consumers are increasingly accessing multiple technology and services to communicate, with 26% of adults in June 2011 using at least four communication technologies, being fixed line telephony, mobile phone, VOIP and the internet.[6]

---

2 Security reforms must protect consumers from increased powers, says Gilbert & Tobin, Communications Day, Decisive Publishing, 28 September 2012, page 6.

3 Proposed data retention laws will leave industry $400m poorer over two years: iiNet, Communications Day, Decisive Publishing, 28 September 2012, page 5.

4 Proposed Security Regime: AMTA, Comms Alliance warn against cost hit for telcos, Communications Day, Decisive Publishing, 28 August 2012, page, 1.

5 Equipping Australia Against Emerging and Evolving Threats, Attorney General's Department, July 2012, p. 18.

- Social media use, again non-existent in 1979 and barely existent at the time of the 2006 reforms to the TIA, has dramatically increased in recent years providing another avenue of communication which needs to be readily interceptable.

The Discussion Paper concludes that many of the legacy assumptions that existed in the 1970s simply no longer apply. Those assumptions included:

- communications to be intercepted are easily identified;
- the stream of traffic to be intercepted can be isolated;
- carriers control the traffic passing over their networks;
- intercepted communications are easily interpreted or understood; and
- there are reliable sources of associated communications information that link people with identifiers and identifiers to communications.[7]

## the legislation is failing to keep up with communications technology and the ingenuity of its users

### The Cybercrime Legislation Amendment Bill 2011

While the overall reform of the telecommunications interception regime will take some time to play out, a number of recent changes are now before the parliament in the form of the Bill and those changes themselves are proving to be controversial.

The changes in the Bill are a further consequence of the increased need for security and reflect the requirement set out in the Council of Europe Convention on Cybercrime (the Convention). Curiously however, at the time of writing Australia has not signed the Convention. Indeed four member states of the Council of Europe have not yet signed the Convention, and an additional eight member states of the Council of Europe have not ratified it. Of the non-member states, only Japan and the United States have ratified the Convention.

There are four main areas of change under the Bill, being the introduction of:

- historic domestic preservation orders;
- ongoing domestic preservation orders;
- foreign preservation orders; and
- foreign law enforcement authorisations.

There are currently no mandated minimum periods for which carriers are required to keep communications information, such as stored communications or call related information (for example, where the call was made, the length of the call and to whom it was made). Depending on the organisation, such communications could be kept by carriers for as little as a couple of hours, or for as long as week. As a result, if an investigation by an enforcement agency into a serious offence is not at a stage where that agency could apply for a stored communications warrant to access information that is stored by the carrier at that particular time, currently it is likely that communications relevant to the investigation may be removed from the carrier's records.

The purpose of the preservation orders introduced by the Bill is to allow enforcement agencies to require carriers to retain communications which may be relevant to an investigation for a serious offence so the enforcement agency may have access to those communications when the investigation has progressed further. This appears to have the effect of creating defacto standard retention periods on all carriers, something which is proving controversial in the considerations of the Parliamentary Joint Committee referred to above.

There are however some restrictions on seeking preservation orders in the Bill which are meant to act as safeguards:

- An enforcement agency must, at the time of obtaining a preservation order, confirm that it intends within a three month period to apply for a stored communications warrant to access the material the subject of the preservation order. The intent is to ensure that enforcement agencies are serious about requiring the information for the purpose of their investigation. However, it should also be considered that investigations may change and the enforcement agency may revise its need for the information at a later date. While there are procedures that relate to the revocation of preservation orders, it still does not relieve the carrier from having to preserve the relevant information in the first place.
- There must be reasonable grounds for suspecting that there are stored communications relevant to the offence being investigated.
- Only one person can be listed on a preservation order, and only one order can be issued in relation to the same person or telecommunications service. However the reference to the same person does not include where the person has a number of pseudonyms.
- The enforcement agency must also address any privacy issues.

A preservation order requires carriers to maintain the integrity of the stored communications during the relevant period. While a carrier can keep the original communication or a copy, carriers must ensure the relevant communications are not edited, deleted or otherwise changed.

Historic Domestic Preservation Orders

A historic domestic preservation order will require the carrier to preserve all stored communications that relate to the person or service specified in the order. The effective period for a domestic preservation order is quite short, being from the time the carrier receives the domestic preservation order until the end of that day. However, it includes all stored communications relating to the preservation order that the carrier still has on its systems.

A preservation order is just that – an order for preservation of the relevant stored communications. A carrier must keep the relevant communications for up to 90 days after the date of the domestic preservation order. If the enforcement agency revokes the order, the carrier may delete the stored communications.

A domestic preservation order can only be given to an authorised representative of the carrier. This is either the Managing Director or secretary of the carrier, or an employee of the carrier authorised in writing by the Managing Director or secretary of the carrier. This is the same process that currently applies for stored communications warrants.

The preservation of the stored communications under a domestic preservation order does not entitle an enforcement agency to access those stored communications. Instead, the enforcement agency must then apply for a separate stored communications warrant (or applicable interception warrant), which is subject to separate criteria. Only once the carrier has received the actual stored communications warrant may the carrier release the preserved information. Indeed, for the carrier to do so without a stored communications warrant would be a breach of its obligations under both the TIA and Part 13 of the *Telecommunications Act 1997* (***Telco Act***).

As a result, once a carrier has received a domestic preservation order it must keep the stored communications it acquired during the relevant period until the first of:

- 90 days after the carrier received the domestic preservation order;

6 Ibid, p. 18.

7 Ibid, p. 20.

**The Discussion Paper concludes that many of the legacy assumptions that existed in the 1970s simply no longer apply**

- the expiry of a stored communications warrant (or interception warrant) in relation to the preserved material; or
- receipt by the carrier of a notice revoking the domestic preservation order.

Ongoing domestic preservation orders

Enforcement agencies will also be able to issue 'ongoing domestic preservation orders' requiring carriers to preserve any stored communications in relation to a specific person or service, not only on the day that order was issued, but also for the next 29 days.

Foreign preservation orders

The Australia Federal Police (***AFP***) will be able to issue 'foreign preservation orders', which reflect requests from foreign countries to obtain certain stored communications which might relate to contraventions of certain foreign laws. A foreign preservation order requires carriers to preserve stored communications in relation to a particular person or service on the day that the foreign preservation order was issued.

As is the case with domestic preservation orders, a carrier cannot disclose the stored communications the subject of the foreign preservation order until it receives a stored communications warrant in relation to those stored communications. However, carriers must preserve the stored communications the subject of the foreign preservation order for up to 185 days after the date of the foreign preservation order.

Foreign law enforcement authorisations

The AFP may also issue authorisations for the disclosure of telecommunications data (being non-content related information, such as time, place and duration of a call) where there has been a request for such information from a foreign country. The scope of the disclosure will depend on the type of authorisation issued by the AFP. The AFP is likely to be able to issue foreign law enforcement authorisations from mid-November 2012.

While there appears to be agreement that reform of the TIA is well overdue, many challenges face the Government as it seeks to balance privacy concerns, the minimisation of the burden imposed on industry in conducting what is essentially a public service, and ensuring that Australia's law enforcement authorities may make use of a powerful tool to enhance domestic and international security. Industry stakeholders and the Government will now await the recommendations of the Parliamentary Joint Committee as it seeks to balance what appear to be multiple competing concerns.

***Shane Barber is a Partner, and Lisa Vanderwal is Special Counsel, in the Sydney office of communications and technology specialist law firm, Truman Hoyle.***


# Link in with CAMLA

Keep in touch with all things CAMLA via the new Communications and Media Law Association LinkedIn group.

You will find information here on upcoming seminars, relevant industry information and the chance to connect with other CAMLA members.

LinkedIn is the world's largest professional network on the internet with 3 million Australian members.

To join, visit www.linkedin.com and search for "Communications and Media Law Association" or send an email to Cath Hill - camla@tpg.com.au

# 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 at 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

## 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)