Communications Law BULLETIN

CAMLA

Communications & Media Law Association Incorporated

Print Post Approved PP: 234093/00011

Privacy Law Reform - Getting the Balance Right

In a presentation to the Communications and Media Law Association on 6 September 2011, Timothy Pilgrim reflected on the status of privacy law in Australia in the context of the work done by the Office of the Privacy Commissioner and developments in the privacy law reform process

I would like to begin by acknowledging the Gadigal peoples of the Eora Nation, the traditional owners of the land on which we meet today, and to pay my respects to their elders, both past and present.

Scott McNeally, co-founder of Sun-Microsystems famously said in 1999 that "You have zero privacy – get over it".

Every day there is a substantial growth in the amount of personal information that is available online, and technology continues to bring new opportunities for information sharing. The phenomenal growth of the internet, e-commerce and the international flow of vast amounts of personal information, able to occur in seconds, has created a brave new world for privacy.

It is interesting to look more recently at what some influential people in the field have said.

Mark Zuckerberg, the founder of Facebook, commented that:

> "…when I got started in my dorm room at Harvard, the question a lot of people asked was why would I want to put any information on the Internet at all?"

But he then went on to say that:

> "…people have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time."[1]

And further that:

> "You have one identity. The days of you having a different image for your work friends or co-workers and for the other people you know are probably coming to an end pretty quickly. "And: "Having two identities for yourself is an example of a lack of integrity."[2]

Eric Schmidt, the Executive Chairman of Google, said in 2010:

> "I don't believe society understands what happens when everything is available, knowable and recorded by everyone all the time. "[3]

Today we are clearly in the midst of a social media revolution in which Facebook alone has 750 million users.

The fact that what you post today may cause grief tomorrow seems to elude many social media enthusiasts, so much so that Eric Schmidt also predicted in 2010 that:

> "…every young person will be entitled automatically to change his or her name on reaching adulthood in order to disown youthful hijinks stored on their friends' social media sites."

So in 2011, this environment, why are we now looking at the potential for the introduction of a statutory cause of action to be enacted through the federal Parliament? Why on two occasions

1 See for example, Bobbie Johnson, 'Privacy no longer a social norm, says Facebook founder' *The Guardian* (Online) Monday 11 January 2010.

2 See for example, Jemima Kiss 'Does technology pose a threat to our private life?' *The Guardian* (Online) Saturday 21 August 2010 available at: http://www.guardian.co.uk/technology/2010/aug/21/facebook-places-google

3 Google and the Search for the Future

Volume 30 Nº 3
December 2011

Inside This Issue:

Contents

recently has Facebook announced changes to its privacy settings in response to its users' concerns?

Interestingly, in further elaborating on Facebook's role in the system, which he said is to reflect what the current social norms are, Mark Zuckerberg has also noted that:

> "a lot of companies would be trapped by the conventions and their legacies of what they've built. Doing a privacy change – doing a privacy change for 350 million users, is not the kind of thing that a lot of companies would do."
>
> "But we viewed that as a really important thing, to always keep a beginner's mind and what would we do if we were starting the company now and we decided that these would be the social norms now and we just went for it."

This evening, I'll ponder only some of these issues, as we wouldn't have time to work through all the possible answers, nor would I be silly enough to think that I even have "the answer".

I'll consider instead where we are now with privacy law in Australia in the context of the work we do in our office, looking at some of the cases that we have been involved with recently, and through developments in the law reform process.

But first a little history.

Warren and Brandeis

In 1890, Samuel D Warren and Louis D Brandeis (who later became a US Supreme Court judge) pioneered the idea of a right to privacy – a right to be "let alone"[4]. This was in response to the emergence of new technologies, such as instantaneous photographs, and the rise of the newspaper enterprise, which, in their words, "have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the house-tops."

Jumping nearly a century later and across the Pacific to Australia, in 1969 Sir Zelman Cowen, an eminent Australian jurist and scholar who was later Governor-General of Australia, delivered the ABC's annual Boyer Lectures.[5]

His series of six lectures – The Private Man – explored the serious threats to individuals arising from the emerging era of computerised information. Sir Zelman observed that:

> "…A man without privacy is a man without dignity; the fear that Big Brother is watching and listening threatens the freedom of the individual no less than prison bars."

In the late 1970s and 1980s, Australia made a conscious decision to consider the legal standing of privacy as a party to the International Covenant on Civil and Political Rights, of which Article 17 states:

> No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

and

> Everyone has the right to the protection of the law against such interference or attacks.

This recognition of privacy as a human right and deserving of the protection of law is one of the reasons why we have the Privacy Act 1988.

This was also the period that saw the then government attempt to introduce the "Australia Card" against much opposition within and outside the Parliament. There were even protest rallies against the proposal.

It is interesting to remember that while the Australia Card proposal was scrapped following a double dissolution election held over the issue, the accompanying Privacy Act was passed through the Parliament in 1988.

4 Louis Brandeis & Samuel Warren," The Right to Privacy," 4 Harvard Law Review 193-220 (1890-91) http://groups. csail. mit. edu/mac/classes/6. 805/articles/privacy/Privacy_brand_warr2. html

The Act at that time only covered Commonwealth Government agencies and Tax File Numbers. It was amended in the early 1990s to cover credit information and then, more significantly, in 2000 the coverage of the Act was extended to cover much of the private sector. This was in recognition of the increasing consumer confidence in e-commerce, and also in an attempt to gain European Union adequacy.

However, the amendments to the private sector had some notable exceptions, including the media and political organisations. And this starts to raise the question of potential gaps in privacy protection.

Then, following a recommendation from the former Office of the Privacy Commissioner and a Parliamentary Committee in 2005, the then Government gave a reference to the Australian Law Reform Commission (ALRC) to review the whole Act in the context of a rapidly changing global and technological environment. This review made 295 recommendations for changing the Privacy Act. But a bit more of that later.

Before I consider why we are seeing a renewed interest in privacy, let's look at what privacy is. The type of privacy covered by the Privacy Act is the protection of people's personal information. However, this is just one aspect of privacy.

Other types of privacy can include territorial privacy, physical or bodily privacy and privacy of your communications. And as these are not covered by the Act, here we see some more potential gaps.

Our enquiries line, for instance, receives numerous calls relating to issues of bodily, territorial and informational privacy that are not covered.

What is Privacy?

The Act defines personal information as "…information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion."

This is a deliberately broad definition and reflects the power holding such information can have on the day-to-day lives of people. In the business context, for example, personal information is often seen as an asset; however, I would say that it is a unique kind of asset.

Whereas an organisation may hold physical assets such as office equipment and photocopiers, if these are lost they are easily replaced. While personal information is undoubtedly an asset for business – it is profoundly different from other types of assets. When it is lost or misused, the consequences for individuals and businesses differ significantly.

For the individual there is:

- the potential loss of control over who knows what about an individual;
- the risk that people can be using the information about them for unwanted contact – and this could be through relatively benign ways such as such as marketing through to more serious physical concerns; and
- vulnerability to the threat of identity theft and fraud and the trouble of changing a raft of details – like credit cards and bank accounts.

There can also be significant problems for individuals in getting the integrity of their identity back.

And for businesses, there is the damage to their reputation.

Just to put identity theft in context:

Professor Iain Morrison, head of Bond University's IT School, recently predicted that more than one million Australians will fall victim to information and computer fraud this year, and that computer fraud will cost $3 trillion around the world in 2011.

Indeed, a Newspoll survey conducted in December last year found 23 per cent of Australian workers have received a phishing scam through a social networking site. Interestingly, another survey of 1200 consumers by technology company Unisys found that Australians are more concerned about identity theft and financial fraud than terrorist attacks.

People were asked if they were more or less concerned about security issues than they were 10 years ago (and remember that 2011 marks the 10th anniversary of the September 11 terrorist strikes in the US). While Australians remain concerned about terrorism, with 42 per cent saying they were more concerned about the risk of airline hijackings and 51 per cent were more concerned about suicide bombs, 76 per cent of Australians were even more concerned about their credit card data being stolen, and 59 per cent about companies losing their personal or financial details.

Unisys Security Program Director John Kendall commented that although concerns about "traditional" national security threats persist, "more contemporary issues…have greater potential immediacy" for most people.

So for the individual, personal information is not just like losing a physical asset that can be replaced. This is why the Privacy Act requires businesses and Australian Government agencies that handle personal information to have robust privacy practices in place. The benefits of having access to personal information come with responsibilities, such as a responsibility to use that information only in ways which the Act allows or the person has agreed to in order to get the service or the product they want.

Mark Zuckerberg, the founder of Facebook, commented that: "…when I got started in my dorm room at Harvard, the question a lot of people asked was why would I want to put any information on the Internet at all?

Privacy in the Headlines

There is no doubt that the News of the World events and the continuing incidents of data breach have sparked a growing interest in privacy. The Office of the Australian Information Commissioner (OAIC) has investigated a range of data breaches in recent years.

High-profile cases include:

- Google, who in May 2010 breached the Privacy Act by collecting unsecured WiFi payload data in Australia using Street View vehicles.
- Telstra, who in a mail-out in October 2010, breached the Privacy Act by misdirecting the personal information of 60,300 customers – a one-off, human error.
- Vodafone, who I investigated earlier this year and found did not have appropriate security measures in place to protect customer's personal information. I was particularly concerned by Vodafone's use of shared logins and passwords for staff and the broad range of detailed personal information available to them.
- Sony Playstation Network My own motion investigation into Sony began in April this year and continues as we examine what happened to the personal data, including credit card details, of more than 77 million users when Sony was hacked into.
- Another case you may have heard about in July was an incident involving a medical laboratory, Medvet, which allegedly resulted in the online publication of the personal details of people seeking paternity and drug tests.

These cases provide an insight into how data breaches can occur. It could be because of:

- human error;
- a failure to comply with obligations in regard to the use and disclosure of personal information;

- a failure to take reasonable steps to protect personal information from misuse and loss or from unauthorised access, modification or disclosure; and/or
- something more insidious, such as when personal information held by a company is stolen or 'hacked' into.

The investigations I have just mentioned are notable because of the large numbers of people affected and the sensitivity of the information disclosed.

As you would expect, there are many other cases of data breach that do not make news headlines.

Data breaches you won't have read about in the press that we have investigated include:

- incidents involving the loss or theft of data sticks, documents and computers containing personal information;
- mail misdirection, particularly mistakes made using email; and
- unauthorised employee access to and misuse of customer information.

We have even had a case where documents containing personal information turned up in the drawers of used furniture sold at auction.

In the last financial year, the OAIC received 56 voluntary data breach notifications (or DBNs), up from 44 in the previous year.

"…A man without privacy is a man without dignity; the fear that Big Brother is watching and listening threatens the freedom of the individual no less than prison bars."

We also initiated 59 own motion investigations – and it is highly likely that among these are matters that should well have been DBNs.

Collectively, these incidents have highlighted the issue of mandatory data breach notification or DBN, one of many of the ALRC's recommendations for reform of Australia's privacy regime.

While there is much public attention given to DBN through media reporting, it is useful to put these kinds of incidents in the context of the OAIC's broader compliance workload. Each year we receive around 1200 complaints and more than 20,000 enquiries – either by phone or in writing.

Current Law and DBN

By way of getting into discussion of the privacy law reform process, I'll just mention where the law stands now for data breaches.

The Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) in the Privacy Act do not impose an obligation on agencies or organisations to notify individuals whose personal information has been compromised.

However, the Act does require that agencies and organisations take reasonable steps to maintain the security of the personal information they hold. Failure to do so constitutes a breach of our current laws. The OAIC recommends notification to affected individuals, and in certain cases, to the Privacy Commissioner, as one of the steps in our best-practice guide to data breach handling that you can find on our website.

Despite the current absence of a legal requirement, it is my view that prompt notification should be considered as a matter of course in any situation where a data breach gives rise to a risk of real and serious harm to the individuals whose information has been disclosed.

It's worth mentioning that calls for mandatory data breach reporting are not new: they go back several years, with the Australian Democrats Senator Natasha Stott-Despoja calling for reform through a Private Member's Bill in 2007.

There is no doubt that data breaches cause concern in the mind of the public and lead to calls for tougher regulation, particularly if there is a perception that organisations are not treating them seriously – or worse, trying to cover them up. Consequently, data breaches pose a serious reputational risk to business.

However, an even greater reputational risk confronts organisations found to be either hiding a breach, or doing nothing about it. This will ultimately impact on consumer trust and make people reluctant to deal with them in the future. This is perhaps one of the reasons why the organisations involved in those high-profile cases I mentioned have been extremely cooperative in working with us to resolve the issues.

Law Reform Process

Data Breach Notification was among 295 recommendations for amendments to the Privacy Act in the 2008 Australian Law Reform Commission *Report 108 – For Your Information: Australian Privacy Law and Practice*, the extensive review into Australia's privacy laws.

Other amendments recommended by this review included:

- a new set of harmonised privacy principles to cover both the public and private sectors;
- provisions introducing comprehensive credit reporting to improve individual credit assessments and supplement responsible lending practices;
- provisions relating to the protection of health information;
- a statutory right to privacy; and
- a review of the exemptions to the Act, including clearer definitions around the scope of the journalism exemption.

Given the size of the ALRC's report, the Government decided to respond in a two-stage process.

A first stage response to 197 of the 295 recommendations contained in the ALRC report was released in October 2009 and the Government is still in the process of implementing these changes.

The first stage covers:

- new privacy principles
- credit reporting provisions
- health provisions
- additional powers for the Commissioner.

Australian Privacy Principles (APP)

We are currently in the process of moving towards a single set of privacy principles covering both the public and private sectors in Australia and an exposure draft of these was released by the Australian Government earlier this year.

The proposed 13 APPs are structured to reflect the information life cycle – from collection, through to use and disclosure and access and correction.

Currently, there is one set of principles covering the Australian, ACT and Norfolk Island Governments and a separate set of principles covering business. A single set of principles will simplify privacy obligations in Australia and reduce confusion and duplication.

This is not without its challenges.

Australian Government agencies have been working with the Information Privacy Principles (or IPPS) for 23 years, while the private sector has been covered by the National Privacy Principles (or NPPS) for only 10.

The new draft principles more closely reflect the wording of the NPPs, so the change for government agencies will be potentially bigger.

They also introduce concepts that government agencies haven't had to consider as part of the IPPs – such as sensitive information and the associated need for consent, and a specific trans-border data flow principle.

Sensitive information

For the first time, for example, there will be specific requirements on the way government agencies can collect sensitive information. Sensi-

tive information is a subset of personal information and is defined to include information relating to:

- race or ethnic origins;
- political opinions and membership of political associations;
- religious or philosophical beliefs;
- membership of a trade union or of a professional or trade association;
- sexual preferences or practices;
- criminal record; or
- health information.

Sensitive information is a particular class of personal information that, if misused, can be particularly damaging to the individual concerned.

Cross border information

While this will be a new concept for the Government sector, the new principle also represents some significant changes to the existing cross border principle that the private sector has been used to for the last 10 years. The new draft principle introduces the concept of accountability. This means that entities will remain accountable for any disclosure of personal information outside Australia, unless one of a number of exceptions applies.

Some organisations have raised concerns about how far this 'chain of accountability' would extend. For example, if an organisation contracted a function to an overseas entity, and so made a cross border disclosure, and that overseas entity then engaged a subcontractor, should the organisation be accountable for the way the subcontractor handles the personal information?

In order to give effect to this provision's intent, it is my view is that the chain of accountability would not be broken simply because the overseas entity engaged a subcontractor. The intent of this Principle is to ensure that people can enforce their privacy rights, even when organisations send their personal information offshore.

New credit reporting provisions

Credit reporting has been regulated under the Privacy Act since the early 1990s. In February this year, the Government released an exposure draft of the new credit reporting provisions, and we support the move to simplify these and make them more user-friendly.

Additional powers

The Government has indicated that it will introduce new laws to strengthen the powers of the Privacy Commissioner.

Under the current Privacy Act, we are unable to impose a penalty on an agency or organisation when we have initiated an investigation on our own motion, without a complainant. Our role is to work with the agency or organisation to ensure ongoing compliance and better privacy practice.

The Government has not yet released exposure draft legislation in this area, but it has stated that it intends to make amendments so that the Privacy Commissioner can:

- make an enforceable determination on an own motion investigation;
- accept undertakings from agencies or organisations and, if necessary, enforce those (through a court); and
- seek (through a court) a civil penalty for serious or repeated offences.

At the end of the day, I would rather not have to use such powers. Our recent experience in relation to the Google Street View and Vodafone cases show how agreed undertakings can operate successfully.

Nevertheless, overseas experience has indicated that regulators with the power to pursue large penalties will often do so. The United States is perhaps the best example of this.

One of the most notorious data breaches in the US was the disclosure by ChoicePoint, a large identification and credential verification organisation, of sensitive information it had collected on 145,000 individuals. In this case, a Federal Trade Commission (FTC) investigation led to the imposition of a $15 million fine.

More recently, the FTC investigated Google when Gmail users were opted in to the new social networking platform 'Buzz' by default and their personal information – including which other Gmail users they interact with most – was made public.

As a result of its investigation and as part of its settlement, the FTC now requires Google to enact a consumer privacy protection program by implementing a comprehensive privacy policy and submitting to privacy audits by independent parties every second year for the next two decades.

Additional powers for the Privacy Commissioner will provide added credibility for enforcement of privacy law, reinforce the significance of privacy compliance, and give everyone an even greater incentive to take privacy more seriously.

the new principle also represents some significant changes to the existing cross border principle that the private sector has been used to for the last 10 years.

Current Exemptions from the Privacy Act

As you are no doubt aware, there are a number of exemptions from the Privacy Act, and this again raises the question of gaps in the system.

I'll now touch on some of these and mention some of the recommendations for reform made by the ALRC – and I should note here that Government is yet to respond to these.

Small business exemption

Generally speaking, small businesses – namely, those with an annual turnover of $3 million or less – are exempt from the operation of the Privacy Act, and it has been estimated that up to 94% of Australian businesses may fall under this exemption.

The small business exemption has been scrutinised by four separate inquiries since 2000, when the Privacy Act was extended to the private sector. The ALRC recommended that the small business exemption should be removed, noting that there would be a need to minimise unnecessary compliance costs on small businesses.

Employee records exemption

While the employee records of public servants have been covered by the Act since 1988, other employee records are not covered by the Act.

These kinds of records contain a great deal of personal information that could cause harm to someone if used or disclosed inappropriately – things like the terms and conditions of employment, salary and leave details, taxation, banking or superannuation affairs as well as the employee's trade union membership.

The ALRC was particularly concerned about the lack of adequate privacy protection for employee records in the private sector. So the ALRC recommended that the employee records exemption should go.

The former Office of the Privacy Commissioner (or OPC) supported this proposal because it strengthens the protection of employees' rights as private citizens and creates greater certainty about rights and obligations for both employers and employees.

We also saw value in eliminating the regulatory difficulties an organisation might face in interpreting the exemption, and also opening up our conciliation-based complaints processes to employees.

Political exemption

The ALRC has called for the removal of the exemption for registered political parties and the partial exemption currently applicable to Australian Government Ministers. The former OPC submitted that privacy protection may be enhanced by requiring political parties to

comply with key privacy principles, but, as with the other exemptions, it remains to be seen what the Government will do on this issue.

The ALRC also recommended amending the Privacy Act to provide that the Act does not apply to the extent, if any, that it would infringe any constitutional doctrine of implied freedom of political communication or parliamentary privilege.

The public's right to know must continue to be balanced against individuals' right to privacy – and we know that what the public is interested in is not necessarily the same as what is in the public interest.

Journalism exemption

And now to the journalism exemption, which will probably be of most interest to you tonight. As you will be aware, the practices engaged in by media organisations in the course of journalism are exempt from the operation of the Privacy Act, provided the organisation meets certain requirements, including being publicly committed to standards that deal with privacy. This exemption is said to promote the public interest in freedom of expression and the free flow of information critical to the maintenance of a democratic society.

However, the ALRC's consultation raised some concerns about the nature and operation of the journalism exemption. Some of these include:

- the broad scope of the exemption;
- the lack of criteria and independent assessment of media privacy standards;
- the adequacy of the regulatory model; and
- the lack of strong enforcement mechanisms in some media sectors.

While the ALRC supported the journalism exemption, it recommended a number of improvements to its application, and I'll now consider some of these.

The ALRC noted that self-regulatory mechanisms do not provide the complete answer to the task of balancing competing public interests in privacy and freedom of expression. The ALRC considered that, unlike for other professionals – for example, financial advisers and lawyers – journalists have no ***requirement*** for formal educational. Nor are there compulsory requirements for accreditation or registration.

In this context the ALRC has recommended that components of the journalism exemption be more clearly defined. First, the ALRC noted that the lack of definition of the term 'journalism' was problematic. It suggested that 'journalism' be defined to limit the scope of the exemption to acts and practices that are associated with a clear public interest in freedom of expression.

Similarly, the ALRC suggested amendments to the definition of the term 'media organisation' – to avoid unnecessary circularity with the 'journalism' definition and to allow flexibility in the provisions as new media platforms continue to evolve.

The ALRC believes these new and changed definitions would address comments made by a number of stakeholders, who in their submissions, questioned whether the proposed definitions would exclude emerging mediums for conducting journalism, such as blogs.

For example:

The Australian Library and Information Association commented that the concept of 'the media' is changing rapidly, and suggested that protection might need to be widened to encompass this broad range of mediums.

The Australian Press Council noted that journalism:

> "…is something more than just the straight reporting of, and commentary on, matters of economics, politics and social developments. Sports, travel, food and leisure, film, music and books, and popular culture are all as worthy of coverage, in the public interest."

The Right to Know Coalition also questioned whether advertisements could be excluded from the definition of journalism, noting that this approach could result in material presented in a news or current affairs story falling within the journalism exemption, but the exemption not applying where the same material is presented in an advertisement for the story.

These are interesting discussions that I am sure will continue as the reform process progresses.

Media Privacy Standards

Another recommendation by the ALRC was a new requirement that media privacy standards must deal 'adequately' with privacy in the context of a media organisation's activities.

In light of the events around the *News of the World*, this is a salient point.

The public's right to know must continue to be balanced against individuals' right to privacy – and we know that what the public is interested in is not necessarily the same as what is in the public interest.

During the ALRC consultation process, some people questioned whether the media privacy standards that exist today are sufficient to guard against breaches of privacy if media organisations or journalists behave irresponsibly.

Most media organisations are subject to a range of **voluntary** industry standards – for example, those developed by the Australian Press Council for the print media – and to regulations made under law – such as codes of practice approved and registered by the Australian Communications and Media Authority (ACMA) in respect of the broadcast media.

However, it has been argued that this regulation does not provide real remedies for individuals whose privacy rights have been affected. In this context, the ALRC has identified a range of options for enhancing the operation of the 'commitment to privacy standards' requirement, including the requirement that media privacy standards deal with privacy in an 'adequate' way.

The ALRC's view is that in order to qualify for the journalism exemption, organisations should be publicly committed to 'adequate' privacy standards that relate to the particular activities undertaken by a media organisation. Public commitment is regarded as an important mechanism to ensure that any standards being relied upon will be robust – while respecting the need for a high degree of media autonomy in order to protect freedom of expression.

To promote regulatory certainty, the ALRC also recommended that clear guidance explaining how the requirement for adequacy would be assessed should be developed by the OAIC in conjunction with the ACMA.

Conclusion

So to wrap up, why does privacy continue to be an issue for people?

Well, it could be put this way: at the end of the day, privacy is about what we think, what we believe and value, what we want and what we want to do… basically, who we are – it is the detail of what makes us unique.

It is also about having the greatest ability to control who gets to know these things about us.

But it can't be an absolute in the society in which we live – and in that sense, privacy law reform is about trying to find the balance.

Thank you.

Timothy Pilgrim was appointed as Privacy Commissioner on 19 July 2010. The full version of the speech presented to CAMLA is available at the website of the Office of the Australian Information Commissioner:
http://www. oaic. gov. au/news/speeches. html

How Should Australian Courts Approach the Use of Live Text-based Communications in Court?

Steve Hind considers the use of live text-based communications in court, as well as the risks posed and the approaches taken towards it in various jurisdictions.

Introduction

Writing extra-judicially in 2006, Spigelman CJ, likened those who were instinctively hostile to new Internet technologies to the Dominican friars who opposed the Germans who brought the printing press to Italy in the late 15th century.[1] Fra Filippo di Strata, he said, thought the Germans were "vulgarising intellectual life", distorting the subtlety of the Latin text and providing the word of God to common people without a priest to intermediate.[2]

the Criminal Bar Association said that with Twitter there is the risk "that often things are tweeted that might have been said, but probably would not have been written, had the person had time to reflect".

Similar attitudes have been expressed in relation to live text-based communication technologies (***LTBC***), especially social networking sites like Twitter and Facebook. The Lord Chief Justice of the United Kingdom, in a Consultation Paper about LTBC released this year (the ***Consultation Paper***) noted that posts on Twitter are often written "in a trivial manner, even when they relate to a serious subject matter."[3] In response to the Consultation Paper, the Criminal Bar Association said that with Twitter there is the risk "that often things are Tweeted that might have been said, but probably would not have been written, had the person had time to reflect".[4]

The use of LTBC in court is a real phenomenon. During the 2009 hearing of *Roadshow Films Ptd Ltd v iiNet Limited (No. 3)*,[5] journalists from ZDNet and *The Australian* tweeted coverage of the trial. Some tweets, it was reported, even provoked chuckles in the gallery.[6] Cowdroy J was said to be "well aware" of the tweeting and had done nothing to stop it.[7] Greens staffer and political blogger Ben Raue tweeted during the New South Wales Supreme Court's hearing of Pauline Hanson's abortive electoral fraud suit this year.[8] Raue said he did not ask for permission to tweet, and that he was one of five people doing so at the time.[9] National Media Director for activist group GetUp!, Paul Mackay, posted Twitter updates while the High Court heard *Rowe v Electoral Commissioner*[10] last year. Unable to bring any device with a sim card into the court, Mackay stepped out to post updates.[11] At least to some extent, the cat is out of the bag.

Although the hostility towards it may be unwarranted, LTBC is not without its risks. This article examines the different types of LTBC, the approaches taken towards LTBC in the United States, the United Kingdom and Canada to date, and the risks posed by LTBC. This article also suggests policy responses in light of the foregoing analysis. Discussion of the challenges that LTBC pose to the law of contempt of court is beyond the scope of this paper.

What are live text-based communications?

Various platforms and methods can be used to transmit text live from court. As the Lord Chief Justice noted in the Consultation Paper, longer battery life and improvements in mobile Internet make it easier than ever to operate smartphones and tablet, netbook or laptop computers in court.[12] Information posted via LTBC can be classified as private, mediated public or direct public.

Private posts include text messages sent from mobile phones, emails to specific addressees and private messages accessible only by selected recipients on Facebook, Twitter and the like. Given that these have an intentionally limited audience, they are less relevant than the following categories.

Mediated posts are those sent by a journalist to an editor before publication. In the case of mediated posts, reporters will gener-

---

1 J.J. Spigelman, 'The Principle of Open Justice: A Comparative Perspective' (2006), 29(2) *UNSW Law Journal* 147, 166.

2 Ibid.

3 Lord Chief Justice of England and Wales, 'A Consultation on the Use of Live, Text-Based Forms of Communications from Court for the Purposes of Fair and Accurate Reporting' (Consultation Paper issued by the Judicial Office for England and Wales, 7 February 2011), paragraph 5.4. ('The Consultation Paper').

4 Criminal Bar Association, 'Response on the Use of Live, Text-Based Forms of Communications from Court for the Purposes of Fair and Accurate Reporting' (Response to Consultation Paper issued by the Judicial Office for England and Wales, 2011).

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

6 Margaret Simons, 'Court reporting in 140 character tweets' *Crikey* (12 October 2009) (http://www.crikey.com.au/2009/10/12/court-reporting-in-140-character-tweets/)

7 Ibid.

8 See, for example: http://mobile.twitter.com/benraue/status/80538250447568896.

9 Interview with Ben Raue (@benraue), conducted via Twitter (18 August 2011).

10 [2010] HCA 46.

11 Interview with Paul Mackay (@plmky), conducted via Twitter (18 August 2011).

12 The Consultation Paper, above n 3, paragraph 2.2.

Various platforms and methods can be used to transmit text live from court.

ally file their copy from court, which an editor then posts online. This only differs slightly from the current situation, where reporters leave court to file their copy by email or telephone, in that it increases the frequency of updates.

Direct public posts are those placed on blogs or social networking sites (for example, Facebook and Twitter) that are potentially accessible by a large audience. This article focuses on public posts because these tend to have the greatest impact on the court process due to their potentially limitless availability.

Some qualifications must be made about what exactly is meant by public. Most blogging platforms enable users to restrict their accounts or posts to approved subscribers (or categories of subscribers). This means that it is rare that a person's status update will actually be available to the world at large.

However, despite the existence of mechanisms to restrict access, it is unlikely that a person would use a private account to tweet from court, particularly where that person is a journalist tweeting for the purpose of broad publication. Tweets sent from open accounts are accessible by anyone with Internet access. Individual tweets have a unique URL, like blog posts, though most people are likely to see a tweet when it appears a Twitter 'feed'.[13]

A Twitter user can 're-tweet' so that the original tweet appears in the feeds of the people who follow their account. It is in this manner that a tweet can be reproduced at an exponentially increasing rate, "so that it may achieve an audience of thousands or even millions very rapidly".[14]

International approaches

Other major jurisdictions are yet to establish firm rules about LTBC. In the United States, the US Judicial Conference has no settled policy, though several federal judges have allowed reporters to tweet from court.[15] Where they have been allowed, in at least one case the reporter was required to sit at the back of the gallery to minimise disruption.[16] Last year, Judge Vaughn Walker allowed Twitter to be used in court while hearing *Perry v Schwarzenegger,*[17] otherwise known as the Prop 8 trial.[18] While covering the trial, reporter Dan Levine, using the handle '@fedcourtjunkie', gathered thousands of followers on Twitter.[19]

The issue for policy makers in the United States is that "historically, case law has generally supported the view that the freedom of press does not include the right to broadcast, record or photograph."[20] As a result, in U.S. v Shelnutt,[21] it was held that tweeting from court was prohibited under Federal Rule of Criminal Procedure 53, which bans broadcasts from court. It has been observed that this decision lacked any analysis of why tweeting is similar or dissimilar to the broadcasting of audio or visual information that previous cases had considered.[22]

The United Kingdom is currently reviewing its approach to LTBC. Courts in the United Kingdom are generally subject to similar principles to Australia courts. Under an Interim Practice Guidance issued in February,[23] mobile phones must be switched off in court but the media may request that they be allowed to use them.[24] Further, in the UK, the *Contempt of Court Act 1981* (UK) requires reporting from court to be "fair and accurate". As a result, the Consultation Paper emphasises that the focus of their inquiry is whether accredited members of the media should be permitted to use LTBC.[25] This approach has been criticised in responses to the Consultation Paper.[26]

The UK Supreme Court is already exempt from bans on audiovisual broadcasting, and it was specifically noted in the Interim Practice Guidance that it rarely hears evidence from witnesses and does not have a jury. Under the policy, LTBC can be used by any person where they are silent and do not cause disruption. Anyone using LTBC must abide by any reporting restrictions imposed by the judge.[27]

Notwithstanding that Canada has a similar legal background to Australia, the use of Twitter in court is already relatively common in Canada, where reporters have tweeted from, amongst other trials, the murder trial of Bandidos motorcycle gang members and the highly controversial murder trial of former army officer Russell Williams.[28] However, the Canadian Broadcasting Commission was denied permission to tweet from the murder trial of filmmaker

The issue for policy makers in the United States is that "historically, case law has generally supported the view that the freedom of press does not include the right to broadcast, record or photograph."

13 A feed is a list of tweets, generated either because everyone has included the same 'hash tag' in the text of the tweet, or because the person viewing the feed has elected to 'follow' the tweets of every user in the feed.

14 Criminal Bar Association, above n 4, paragraph 24.

15 Lynn Marek, 'Judges Split on Courtroom Blogging, Twitter Use', *The Connecticut Law Tribune*, 16 March 2009.

16 Ibid.

17 704 F. Supp. 2d 921 (N.D. Cal. 2010).

18 Adriana C. Cervantes, ' Will Twitter Be Following You in the Courtroom?: Why Reporters Should Be Allowed to Broadcast During Courtroom Proceedings' (2011) 33 *Hastings Communication and Entertainment Law Journal* 133, 135.

19 Ibid, 135.

20 Ibid, 137.

21 No. 4:09-CR-14 (CDL). Nov 2, 2009.

22 Cervantes, above n 18, 149.

23 The Supreme Court of the United Kingdom, 'Policy on the Use of Live Text-Based Communications from Court', (Interim Practice Guidance, The Supreme Court of the United Kingdom, February 2011). ('The Interim Practice Gudiance').

24 Ibid.

25 The Consultation Paper, above n 3, paragraph 1.

26 Criminal Bar Association, above n 4, paragraph 13; British and Irish Legal, Educational and Technology Association, 'Response to the consultation by the Judicial Office of England and Wales on the Use of Live, Text-Based Forms of Communication from Court for the Purposes of Fair and Accurate Reporting' (Response to Consultation Paper issued by the Judicial Office for England and Wales, 2011).

27 Ibid.

28 'Too much tweets? Some loathe, some love Twitter courtroom coverage', Alexandra Zabjek, Postmedia News, 21 March 2011.

the use of Twitter in court is already relatively common in Canada, where reporters have tweeted from, amongst other trials, the murder trial of Bandidos motorcycle gang members

Mark Twitchell.[29] Notably, in the Williams case, the reporter worked in court with an editor next to her so that they could discuss their approach to sensitive parts of the evidence and argument.[30]

The principles of open justice

Earl Loreburn said in *Scott v Scott*,[31] "the inveterate rule is that justice shall be administered in open Court".[32] A 'corollary' of the public's right to attend court is their right to report what is seen and heard in open court, and this right is not limited to the media.[33] In approving the House of Lords' decision in *Scott*, Gibbs J stated in *Russell v Russel*[34] that:

> [t]his rule has the virtue that the proceedings of every court are fully exposed to public and professional scrutiny and criticism, without which abuses may flourish undetected. Further, the public administration of justice tends to maintain confidence in the integrity and independence of the courts.[35]

This year, French CJ said in *Hogan v Hinch*[36] that:

> [t]he open hearing is an essential characteristic of courts, which supports the reality and appearance of independence and impartiality. Its corollary is the freedom to make a fair and accurate report of what transpires in court proceedings…[37]

LTBC offer the press and members of the public a powerful way to exercise their right to report on what they see and hear in court. In doing so, they spread the benefits of that publicity that Gibbs J and French CJ highlighted.

When considering the challenges posed by LTBC, the question should be whether there are grounds to infringe on the principle of open justice, rather than whether this new form publicity should be allowed. A response to the Consultation Paper suggested that by asking whether there was a legitimate demand for the use of LTBC, the Lord Chief Justice miscast the question. Instead he should have asked whether there was a legitimate basis upon which to ban it.[38] This section considers the various justifications for banning or regulating the use of LTBC.

The power to exclude the public

The first exception to open justice that must be examined is the right of judges to exclude the public from court. In *Scott*, the Earl of Halsbury said that the public, or some members of it, could be excluded from court where:

> [t]he administration of justice would be rendered impracticable by their presence, whether because the case could not effectively be tried, or the parties entitled to justice would be reasonably deterred from seeking it at the hands of the Court.[39]

In that case, Viscount Haldane LC said that a court could not sit in camera "unless it be strictly necessary for the attainment of justice".[40] The *Federal Court of Australia Act 1976* (Cth) establishes this principle for federal courts in section 17(1).

While Parliament has the power to require some hearings be held in camera, it cannot completely do away with the principle of public courts. In *Russell*, the court was asked, inter alia, to consider the constitutional validity of section 97 of the *Family Law Act 1975 (Cth)* which provided that family law proceedings be heard in closed court. In holding that it was invalid, Gibbs J said that while the "category of…exceptions is not closed to Parliament", the requirement that all hearings be held in camera was an attempt by Parliament "to obliterate one of [courts'] most important attributes."[41]

Of course if a court is cleared, it will not matter whether the ejected public are using Twitter. More relevant is the power of courts to exclude certain people and to make non-publication, pseudonym and suppression orders.

Power to exclude certain individuals

The power to exclude certain individuals from court was well summarised by Bowen CJ in *Australian Broadcasting Corporation v Parish*.[42] Witnesses can be excluded so they do not "trim their evidence" as can "demonstrators or rioters" who may disrupt proceedings.[43] The categories are not closed and the discretion will lie with the judge, taking into account the principle of open justice.[44]

When considering the challenges posed by LTBC, the question should be whether there are grounds to infringe on the principle of open justice, rather than whether this new form publicity should be allowed.

---

29 Ibid.

30 Ibid.

31 [1913] AC 417.

32 Ibid, 445.

33 *Raybos Australia Pty Ltd v Jones* (1985) 2 NSWLR 47, 55 (Kirby P).

34 (1976) 134 CLR 495.

35 Ibid, 520.

36 [2011] HCA 4.

37 Ibid, [46].

38 British and Irish Legal, Educational and Technology Association, 'Response to the consultation by the Judicial Office of England and Wales on the Use of Live, Text-Based Forms of Communication from Court for the Purposes of Fair and Accurate Reporting' (Response to Consultation Paper issued by the Judicial Office for England and Wales, 2011), paragraph 2. ('BILETA Response')

39 *Scott v Scott*, above n 31, 446.

40 Ibid, 437.

41 *Russell v Russell*, above n 34, 520.

42 (1980) 43 FLR 129.

43 Ibid, 132.

44 Ibid.

Reporting restrictions such as suppression, non-publication and pseudonym orders all modify the principle of open justice and, specifically, the right of people to report on what they see in open court.

In the Consultation Paper, the Lord Chief Justice saw a risk of disruption in interference by mobile internet with the court's amplification and sound recording equipment, and by having a gallery full of people using phones and computers that may ring, make noises or be noisy to use.[45] In a response to the Consultation Paper, a group of information technology law academics said that in their experience there was a "high likelihood" that courtroom speakers would suffer from interference,[46] and a room full of people typing on noisy laptop keyboards could be disruptive.[47] Lord Chief Justice's Interim Practice Guidance on the LTBC in December 2010 said the number of people using the technology could be limited solely on the potential for disruptions of this kind.[48]

It seems unduly restrictive to ban LTBC purely because of the risk of noise or audio interference. Instead a judge could adopt an approach taken recently in the United States and request that those using LTBC sit at the back of the gallery.[49] More generally, judges could monitor any disruption and only require that LTBC not be used in the event that the disruption significantly impairs the proceedings.

Reporting restrictions, witnesses and jurors

Reporting restrictions such as suppression, non-publication and pseudonym orders, all modify the principle of open justice and, specifically, the right of people to report on what they see in open court. They also prevent those present in court from reporting on names, identities, information evidence that is disclosed in open court. Understanding why these orders are made will be useful in showing how that rationale can be extended to support different orders or legislation aimed at limiting the risks associated with LTBC.

The High Court considered the validity of suppression orders this year in *Hogan v Hinch*. Considering some conflicting authority, French CJ concluded that there was inherent jurisdiction to restrict publications but that the power must be justified by reference to what is necessary in the interests of the administration of justice.[50] This mirrored the tests proposed by McHugh JA in *John Fairfax & Sons Pty Ltd v Police Tribunal of New South Wales*[51] and by Mahoney JA in *John Fairfax Group Pty Ltd (Receivers and Managers Appointed) v Local Court of New South Wales* (1991).[52]

The utility of such orders and the reason why they fit with the logic of the principle of open justice was explained by Lord Widgery CJ in *R v Socialist Workers Printers and Publishers Ltd.*[53] Orders that control what can be published mean that the presence of the public can still supervise and impose discipline on the courts, without the risk that the administration of justice will be frustrated in ways that might otherwise justify hearings being held in camera.

Legislatures across Australia have granted judges statutory powers to make suppression orders. The resulting powers are, in the words of some commentators, "too numerous and various to mention".[54] French CJ confirmed in *Hogan v Hinch* that a statutory discretion to make suppression orders would be unlikely to deprive the court "of an essential characteristic of a court."[55]

Legislation conferring a power to make suppression orders to deal specifically with risks posed by LTBC would be of limited utility. The relevant issue is not whether an order should be made but how its terms should be crafted and conveyed in the presence of those using LTBC. Legislation that permits judges to make such orders, or that specifies the manner in which such orders should be made,[56] would be otiose as judges are well aware of the existing principles governing the making of such orders.

To understand how such orders can be crafted to mitigate risks of LTBC, it is necessary to lay out the risks posed. These can be divided into three broad categories: the live reporting of evidence that is later contradicted or ruled inadmissible, witnesses seeing reports of testimony of other witnesses, thereby allowing them to 'trim their evidence', and jurors accessing and reading reports of evidence that may not be admissible. In analysing these risks two questions must be asked. First, to what extent are these risks increased by LTBC in court? Second, to what extent can those risks be managed by judicial orders?

Live reporting of evidence

As the Lord Chief Justice noted in the Consultation Paper, sensitive information frequently emerges during trial without its sensitivity being immediately apparent. Where this occurs, a judge may subsequently ask the media to omit such information from their reports.[57] However, the response to the Consultation Paper by the British and Irish Law, Education and Technology Association[58] notes that in the case of live reporting of evidence that may later be contradicted or ruled in admissible, damage to the reputation of

The relevant issue is not whether an order should be made but how its terms should be crafted and conveyed in the presence of those using LTBC.

45 Ibid.

46 BILETA Response, above n 38, 3.

47 Ibid, 5.

48 Interim Practice Gudiance, above n 26, paragraph 15(b).

49 Lynn Marek, 'Judges Split on Courtroom Blogging, Twitter Use', *The Connecticut Law Tribune*, 16 March 2009.

50 Ibid [26].

51 (1986) 5 NSWLR 465, 476.

52 26 NSWLR 131, 161.

53 [1975] Qb 637.

54 David Rolph, Matt Vittins and Judith Bannister, 'Media Law: Cases, Materials and Commentary' (2010) *Oxford University Press*, 401.

55 *Hogan v Hinch* [2011] HCA 4, [27].

56 See, for e.g. *Court Suppression and Non-Publication Orders Act 2010* (NSW).

57 The Consultation Paper, above n 3, paragraphs 6.1-2.

58 ('BILETA').

LTBC does not necessarily create a new risk, but may increase the scale of the existing risk.

witnesses and other individuals, and even damage to the share price of companies may already have occurred by the time such a direction is given.[59]

These risks are clearly associated specifically with the live reporting of evidence. BILETA's suggested solution is for judges to direct those engaging in LTBC not to report until after the examination in chief, cross examination and (where appropriate) re-examination have taken place.[60] A more flexible approach would be for such orders to apply for either all testimony in a case or for particular witnesses, as the circumstances may dictate. Judges could then direct the gallery as to what information, if any, should be withheld from reports. This solution will not prevent every instance in which sensitive information may be broadcast, but it would minimise such instances while allowing more detailed reporting of testimony. Reporters, one imagines, would draft a series of tweets or draft articles and then publish them once the testimony is completed and any necessary changes have been made.

Witnesses 'trimming their evidence'

Judges may require that witnesses not be present in court before they testify. This prevents witnesses hearing the evidence of others and thereby "trimming their evidence."[61] LTBC enables witnesses to easily read the testimony of others online, creating a situation that is the same in effect as if they were present in court.[62]

In this situation, LTBC does not necessarily create a new risk, but may increase the scale of the existing risk. Suppression orders aside, there is nothing to stop a person exiting a courtroom and communicating what they have heard inside to anyone else, including future witnesses.

LBTC therefore makes it easier for nefarious witnesses to trim their evidence and it also increases the chance that witnesses may be influenced by reports of other evidence. While little can be done to stop people intent on trimming their evidence, clear directions to witnesses that they are not to investigate online reports of the trial before they testify could mitigate many of the remaining risks.

Jurors accessing online reports

The problem posed by jurors using the Internet and internet-enabled devices in court and during their deliberations has received academic attention in the United States.[63] Preventing jurors from accessing the Internet seems futile. Instead we should ask whether, given that the risk of Internet use by jurors exists, LTBC make the problem unmanageable.

LTBC has the potential to allow increasing amounts of detailed information to be accessed by jurors in the event that they decide to ignore the directions given to them.

Although jurors are informed by the judge not to conduct independent Internet research,[64] LTBC has the potential to allow increasing amounts of detailed information to be accessed by jurors in the event that they decide to ignore the directions given to them. Since any independent investigations by jurors can render a conviction unsafe,[65] banning LTBC to reduce the amount of information available would not necessarily prevent a mistrial. Again it seems the more effective and proportionate approach would be to give juries clearer and more detailed directions that clarify that they are to avoid researching the case on social networking sites. Spigelman CJ has noted extrajudicially that in Australian courts "there is a greater faith in the ability to ensure a fair trial by means of strong directions" to juries.[66]

Conclusions and recommendations

The use of LTBC in court provides opportunities to engage the public in the business of the courts. However it may also pose risks to the operation of the legal system if it continues unregulated. Given that an outright ban is unlikely to prevent some of the contemplated harms, clear judicial directions and guidance will be necessary. These should encompass how, when and where LTBC can be carried out. Provided that these are sufficiently clear, it may not be necessary to require those engaging in LTBC to nominate themselves, sit in a special area or seek individual permission as is suggested in the Consultation Paper.[67]

Perhaps more importantly, the courts should consider how they communicate with the public about how they may use LTBC in court. Clear and accessible instructions about the rules and procedures should be posted online. Although none of these measures will avoid all problems or mitigate all risks, they should manage those risks sufficiently well to allow LTBC to be used in court.

Steve Hind recently completed a Bachelor of Laws at the University of Sydney, where he has also completed a Bachelor of Economics.

59 BILETA Response, above n 23, 3-4.

60 Ibid, 2.

61 *ABC v Parish* (1980) 43 FLR 129, 132.

62 The Consultation Paper, above n 3, paragraph 4.5.

63 See Frederic, I. Lederer, 'Wired: What We've Learned About Courtroom Technology' (2010) 24 *Criminal Justice* 18.

64 See *Regina v Bilal Skaf* [2004] NSWCCA 37, [280].

65 Ibid, [242]–[277].

66 Spigelman, above n 1, 164.

67 Above n 3.

Museums and Web 2.0: Mission-Driven Approaches, Legal Challenges and New Opportunities**

Susan Sheffler examines the integration of Web 2.0 practices by museums and some of the legal challenges they face in digitising their collections.

Introduction: Museums and the Internet, Unlikely Bedfellows?

In January 2009, the Smithsonian Institution, a national museum conglomerate of dozens of individual institutions with 137 million physical objects, 6000 staff members and a $1.2 billion annual operating budget, hosted a conference entitled Smithsonian 2.0 as an effort to explore "how to make SI collections, educational resources, and staff more accessible, engaging, and useful to younger generations."[1] What followed were months of hard work and collaboration between Smithsonian staff, external stakeholders, and the internet community at large. This work included a series of public wiki articles used to draft a Web and New Media strategy for the Smithsonian. How did one of the largest national cultural institutions in the world come to embrace such a collaborative model for strategic planning?

The shift during the last decade from Web 1.0 experiences to Web 2.0 communities has contributed to a parallel shift in museum culture and efforts at audience engagement. Over the past 20 years, there has been a move away from traditional museum methods of communication (curator designed exhibits unilaterally conveying a single message to visitors) to a collaborative and multi-directional model in order to make museums more relevant, effective, and engaging.[2] With this goal in mind, museums have actively pursued increased access to their collections and interactivity both on their own websites and on third-party platforms like YouTube, Facebook, and Twitter.[3] These entrances into the digital world have demanded collaboration both inside and outside of the museum, engaging multiple departments and levels of staff, community stakeholders and other cultural groups and institutions with similar missions and audiences.

This paper explores the mapping of old missions and activities onto a digital framework for digital natives, potential problems when digitising collection holdings such as copyright issues and treatment of those orphaned works and collection items that are in the public domain, and innovative attempts to bring Web 2.0 principles back inside the museums' galleries.

Museum Missions in a Digital Age

Traditionally, museum missions, especially those founded during the 19th and early 20th centuries, have focused on the collection, preservation and faithful stewardship of objects of artistic, historical, scientific and cultural importance. This mission has been manifested through a one-way transmission of information from museum expert (including curators, docents and educators) to visitors. One need only look to the Metropolitan Museum of Art, whose canonical mission conjures the image of a museum slavishly purchasing and protecting its collection and monolithically interpreting and presenting it for the public good.[4] The focus of a visit to these grand institutions is on the authenticity and rarity of the objects on display, explicated by the expert voice of the museum as a whole, backed by the scholarship of the curator.

The shift during the last decade from Web 1.0 experiences to Web 2.0 communities has contributed to a parallel shift in museum culture and efforts at audience engagement

In contrast, Web 2.0 disperses authority and creativity and eschews transmission in favour of collaboration. Users of Web 2.0 sites are not simply visitors but also participants, judging and selecting content based on their individual preferences and needs.[5] Even before the dawn of Web 2.0 initiatives, new museology, beginning in the late 1970s and early 1980s, had started turning away from the traditional focus on collecting, researching, and curating,[6] towards education and communication with audiences. Newly evolving mission

---

**** Editors' Note: This article is an analysis of the experience in the United States of America and while some of the issues it discusses are of general application it does not purport to consider the issues as they apply to the Australian context.**

1 Edson, M., et. al., Fast, Open, and Transparent: Developing the Smithsonian's Web and New Media Strategy, In J. Trant and D. Bearman (eds). MUSEUMS AND THE WEB 2010: PROCEEDINGS. Toronto: Archives & Museum Informatics. Published March 31, 2010. Available at http://www.archimuse.com/mw2010/papers/edson/edson.html. (Hereinafter "Edson").

2 Simon, Nina, *Discourse in the Blogosphere: What Museums Can Learn from Web 2.0*, Museums & Social Issues, Vol 1, No 2, Fall 2007, 257. (Hereinafter "Simon."); Jeffrey P. Cunard, Debevoise & Plimpton LLP, Developing and Distributing Museum Content: Navigating the Sea of New Apps, Platforms, and Hosting Options at ALI-ABA Conference: Legal Issues in Museum Administration (March 22, 2011). (Hereinafter "Cunard")

3 *See e.g.* Cunard; Lagoudi, E. and C. Sexton, *Old Masters at Your Fingertips: the Journey of Creating a Museum App for the iPhone and iTouch*, In J. Trant and D. Bearman (eds). *Museums and the Web 2010: Proceedings.* Toronto: Archives & Museum Informatics. Published March 31, 2010, Available at http://www.archimuse.com/mw2010/papers/lagoudi/lagoudi.html.

4 The mission statement reads: "The mission of The Metropolitan Museum of Art is to collect, preserve, study, exhibit, and stimulate appreciation for and advance knowledge of works of art that collectively represent the broadest spectrum of human achievement at the highest level of quality, all in the service of the public and in accordance with the highest professional standards." Metropolitan Museum of Art. About: Mission Statement. Available at http://www.metmuseum.org/about/

5 O'Reilly, Tim, *What is Web 2.0? Design Patterns and Business Models for the Next Generation of Software*, O'Reilly, 30 Sept 2005, available at http://oreilly.com/web2/archive/what-is-web-20.html.

6 Ramesh Srinivasan, et. al. *Digital Museums and Diverse Cultural Knowledge: Moving Past the Traditional Catalog*. 25 The Information Society 4, 265, 266-67. Available at http://www.informaworld.com.ezp-prod1.hul.harvard.edu/smpp/content~db=all?content=10.1080/01972240903028714.

Web 2.0 disperses authority and creativity and eschews transmission in favour of collaboration

statements like that of the Brooklyn Museum[7] mirror this fundamental shift from the role of museums as object collectors and protectors to knowledge creators and collaborators. These institutions with new visitor and education-centred missions have often also been at the forefront in embracing digital technologies, digitisation and Web 2.0 approaches both online and in the galleries.

Several tensions exist between the values that underpin the traditional museums' culture and experience and those that drive online innovation and collaboration. One major value underlying museum collection and exhibition is the authenticity and the uniqueness of the collection objects. The internet, in contrast, values that which is easily reproducible and transferrable, shirking authenticity for access. However, authenticity is not a value that museums are likely to surrender, since it is foundational and ensures their survival. The ideal solution would therefore be a marriage of the online museum experience with the in-person experience, allowing users to access targeted information before their in-person experience, visiting and connecting with authenticity and museum expertise in an open dialogue during an actual visit, and enriching the visit after the fact by allowing online comments, dialogue and further exploration.

Another conflicting value is museums' general resistance to change. Museums have succeeded thus far by focusing on preservation and conservation. In contrast, much of Web 2.0 thrives on a social entrepreneurship model which can start small and expand, changing swiftly to suit users demands and needs[8]. Museum practitioners who are attempting to integrate Web 2.0 practices have encouraged museums to embrace innovation and flexibility through a model of "continuous iterative design, build[ing], testing, refin[ing]".[9] In this redefined model of museums as institutions of social entrepreneurship, there must also be fundamental changes in the top-down management structure of museums with more collaboration between departments. One strategy for encouraging this kind of collaboration is the formation of new "border habitats" – areas where the activities and responsibilities of departments in the compartmentalized museum[10] overlap; for example, promoting direct collaboration between the IT, communication, and curatorial departments to build content for the museum's website. Within these "border habitats," staff can both envision and seamlessly implement their ideas, bringing the museum closer to becoming a flexible and adaptive organization.

Despite these underlying tensions, there are many ways in which traditional museum missions and work can be augmented by cyberspace. For example, digitisation encourages access to collections by the broadest possible audience, which assists museums in fulfilling their role of "serving" and educating the public.[11] Increased connectivity also opens up new avenues for collaboration, independent of geography. Online Web 2.0 tools like wikis have revolutionized the methods of collaboration with other institutions with similar values. While, at first glance, museum values like authenticity may seem to be antithetical to the values and norms of cyberspace, there is potential for museums to expand the reach of their missions when the two sets of values are innovatively integrated.

Problems and Possibilities in Digitising Collections

Copyright and Museum Digitisation

The copyright issues faced by museums in digitising their collections are as diverse as the collections themselves.[12] While many of the works in a museum's collection, particularly where that collection has a historical focus, are in the public domain, museums that collect art and objects from the early 20th century and onwards will need to deal directly with copyright holders in order to obtain a licence for reproduction and display online.[13] A hard line must therefore be drawn when examining potential legal liability between objects in the collection that are in the public domain or not copyrightable and those that may still fall under copyright protection, including orphaned works.[14] The two options available to museums for copyrighted works are either negotiating licences on an individual basis with copyright holders, or relying on copyright exceptions like fair use.

Difficulties associated with pursuing the licensing option include the painstaking task of seeking out licences for each individual work from individual copyright holders, the high costs that may be associated with these licences, and the numerous individual restrictions and conditions that may flow from these licences. For example,

Museum practitioners who are attempting to integrate Web 2.0 practices have encouraged museums to embrace innovation and flexibility through a model of "continuous iterative design, build[ing], testing, refin[ing]"

---

7 The mission of the Brooklyn Museum is to act as a bridge between the rich artistic heritage of world cultures, as embodied in its collections, and the unique experience of each visitor. Dedicated to the primacy of the visitor experience, committed to excellence in every aspect of its collections and programs, and drawing on both new and traditional tools of communication, interpretation, and presentation, the Museum aims to serve its diverse public as a dynamic, innovative, and welcoming centre for learning through the visual arts. Brooklyn Museum of Art. Mission Statement. Available at http://www.brooklynmuseum.org/about/mission.php.

8 Edson

9 *Id*.

10 *Id*

11 *See* Metropolitan Museum of Art. Mission Statement, *supra* note 4.

12 Museums' copyright troubles are further exacerbated by the fact that few museums are large enough to have in-house counsel or budgets for hiring outside counsel to assist them in understanding copyright regimes. Instead, research into copyright liability often falls to professional staff, typically librarians/archivists. Museums and libraries with digitisation projects, according to a 2008 survey, spent an average of over 221 hours/year obtaining rights permissions and copyright clearance while only 3.45% of these institutions have been able to outsource copyright management programs to a third party. *See* International Survey of Library & Museum Digitisation Projects Presents Data from More than 100 Library [sic] and Museums. Artdaily. http://www.artdaily.com/index.asp?int_sec=2&int_new=25872; Primary Research Group, Dec 2010, *The Survey of Library & Museum Digitisation projects 2011 Edition*, Press Release/Description. Available at http://www.researchandmarkets.com/product/26199f/the_survey_of_library_museum_digitisation_p. *See also* Deborah Wythe, Brooklyn Museum, Rights Transparency: The Brooklyn Museum Copyright Project, at ALI-ABA Conference: Legal Issues in Museum Administration (March 22, 2011). (Hereinafter "Wythe").

13 17 U.S.C.A. § 107(1) (2007). *Id*. §106(5) (2007).

14 Orphaned works are those whose copyright holder is unknown and is either difficult or impossible to find. *See* **UNITED** STATES COPYRIGHT OFFICE, REPORT ON ORPHAN WORKS, (Jan. 2006), *available at* http://www.copyright.gov/orphan/orphan-report.pdf.

digitisation encourages access to collections by the broadest possible audience, which assists museums in fulfilling their role of "serving" and educating the public

while larger organizations like ARTstor.org have found success with the licensing method, access remains a key concern as ARTstor has found it necessary to prohibit any online (even non-commercial) use of the images it houses and to restrict access to the database to only those affiliated with a subscribing non-profit institution.[15]

Given their public, cultural and educational missions, museums would seem to be strong candidates for copyright statutory exemptions and limitations. However, the two main exemptions applicable to museums, reproduction for preservation by libraries and fair use, are shaky in application.[16] For the first exception, the Digital Millennium Copyright Act (***DMCA***) expanded the narrow exception from §108 of the 1976 Federal Copyright Act for libraries and archives to include digital copies necessary for preservation and replacement.[17] However, §108 still fails to address public access to digitisation that has been undertaken for the purpose of preservation, which makes it an unsatisfactory legal tool for museums which desire to both preserve and make accessible their collections.[18]

A more expansive statutory exemption available to museums is the affirmative defence of fair use. However, the lack of a bright line rule on what constitutes fair use makes museums, with their tight budgets and limited access to legal resources, reluctant to digitise any items in the collection which may lead to copyright infringement claims.[19] Additionally, museums may find it difficult to pass the four factor test[20] based on the substantiality of the copying of the original that is inherent in digitisation and the potential effect on the market for digital reproductions of artworks, as seen in the licensing-focused models of ARTstor and Getty Images.[21] Museum collection digitisation would also likely fail the "transformative" test that is frequently used in current case law and which disfavours use of copyright material that does not independently "stimulate creativity."[22]

Despite these barriers, museums have found an exception supported by case law which has allowed them to move forward: fair use of thumbnail images. The use of thumbnail images has repeatedly been held to be fair use based on the relatively small amount of the original work that has been appropriated (factor three).[23] While the thumbnail exception is useful for progressing digitisation projects, museums' missions, focused on the preservation of, access to, and education through their collection, are not best served by the sole use of thumbnails in their digitisation efforts. Larger, high-resolution images are an integral part of providing true access to these works for both researchers and larger audiences. Fair use remains an ambiguous area for museum digitisation, thwarting progress to move the vast collections and expert knowledge of museums online where they may be preserved for and accessible to the world.

The Brooklyn Museum: Using Licensing Agreements to Digitise Works still under Copyright

The Brooklyn Museum has worked diligently to offer full records and photographs of the artworks in its collection online. Currently, over 95,000 works are available in this database and each contains a specific rights statement.[24] These rights statements assist the museum in classifying the copyright status of works in its collection and educate the museum's online audience of the nature of copyright.[25] The museum has attempted to find a balance between "the intellectual property rights of others"[26] and the Digital Lab's mission to "create, manage, make accessible and preserve digital images documenting the museum collections, research resources, and activities."[27] In striking this balance, the museum has become a leader in the museum digitisation field, working arduously to educate both the public and other museums on how to implement a digitisation pro-

museums that collect art and objects from the early 20th century and onwards will need to deal directly with copyright holders in order to obtain a licence for reproduction and display online

15 Guy Pessach, *Museums, Digitisation and Copyright Law – Taking Stock and Looking Ahead*, 1 Int'l Media & Ent. L. 253, 261. (Hereinafter "Pessach.")

16 Pessach at 264.

17 *See* Pessach at 264. *See also* The Digital Millennium Copyright Act (DMCA),, Pub. L. No. 105-304, §§ 103,

1201, 112 Stat. 2860, 2863-65 (1998) (codified as amended at 17 U.S.C. §§ 103, 1201

(2000)).

18 *Id*. at 267.

19 *Id*. at 269-70. This reluctance could result in a dearth of public access to and scholarship about periods still covered by copyright, including modern and contemporary art.

20 Four factor test for fair use: **(1)** the purpose and character of the use,

(2) the nature of the copyrighted work,

(3) the amount and substantiality of the portion used, and

(4) the effect of the use on the potential market for or the value of the copyrighted work. 17 U.S.C.A. §107 (2000)

21 Pessach at 269-70.

22 Pierre N. Leval, *Toward a Fair Use Standard*, 103 Harv. L. Rev. 1105, 1111.; *See also* Pessach at 271.

23 *See* Pessach at 271-73; *Bill Graham Archives LLC. V. Dorling Kindersley Ltd.*, 386 F.Supp.2d 324 (S.D.N.Y. 2005), *aff'd*, 448 F.3d 605 (2d Cir. 2006); Kelly v. Arriba Soft Corp., 336 F.3d 811 (9th Cir. 2003); Cf. *Perfect 10 v. Google, Inc., et al.*, 416 F.Supp.2d 828 (C.D. Cal. 2006), *reversed* (to uphold thumbnail image use by Google as fair use) 508 F.3d 1146 (9th Cir. 2007). In *Perfect 10*, some of Google's activities were found to be infringing based on Google's profit through ad revenue, and an impact on the market for thumbnail sized images for use on cell phones. It is unlikely that either of these infringing activities would be found in the museum digitisation case; however, it is worth considering the potential for an expanded market in thumbnail images for cell phone use. *Id.* at 832.

24 *See e.g.* http://www.brooklynmuseum.org/opencollection/objects/4885/Portrait_of_Madame_Tallien

25 *See* Brooklyn Museum, *About: Copyright*. Available at http://www.brooklynmuseum.org/copyright.php. All of the museums rights statements use a minimum of legalese and are largely in plain language. This may owe to the fact that they were written by non-lawyers with a minimum consultation with pro bono outside counsel. Wythe talk/paper at ALI-ABA.

26 Brooklyn Museum, *About: Copyright*. Available at http://www.brooklynmuseum.org/copyright.php

27 Wythe.

air use remains an ambiguous area for museum digitisation

gram which incorporates accessibility, clear notice to audiences of known and potential copyright claims in digitised works, accurate record-keeping of all rights holders, and an open and relatively inexpensive licensing program.[28]

The Brooklyn Museum has adopted a two-pronged approach to digitisation of works of art that are not in the public domain. First, administrators have chosen to continue with the digitisation project, and, second, the Department of Digital Collections and Services has sought out the original artists in order to obtain licences for each of these copyrighted works. In order to ensure that digitisation efforts do not lead to copyright infringement liability, the Head of Digital Collections and Services, Deborah Wythe, has taken extensive measures to find rights holders and send letters to artists represented in the Brooklyn Museum's collection which include a non-exclusive licence to allow the museum to reproduce, display, transmit, publish, and distribute images of the artist's work in ways which "fulfil its mission" and are "related to the museum's collection and programs."[29] The museum has an involved process for locating rights holders (particularly in relation to lesser known and orphaned artworks), which focuses on locating the artist, their heirs, and other stakeholders such as the artists' galleries. While awaiting the outcome of these licence requests, the museum only makes thumbnails of the work available online, explaining in the rights statement for these objects that "copyright to this work may be controlled by the artist, the artist's estate or other rights holders."[30] Once a non-exclusive licence agreement is returned,[31] the museum makes the full-sized image of the artwork available in the online database.

Reactions to the Brooklyn Museum's digitisation methods and licensing scheme have generally been positive, but the program has still faced several difficulties, particularly in relation to orphaned works. Research into the rights status of orphaned works takes into account in-house archives, curatorial notes, and artist files, professional associations, rights holders' organizations, publications, and gallery and auction house databases.[32] If, following this research, the museum is still unable to locate the rights holders, the museum makes full sized images of the works available with a corresponding rights statement.[33]

While this approach exposes the museum to copyright infringement liability, it represents an active choice by the museum to favour accessibility over complete freedom from liability. The request for further information on rights to the work also has the potential to engage audiences and rights holders in a dialogue with the museum, promoting goodwill that can both legitimize what the Brooklyn Museum and others like it are doing as well as lessening animosity, and therefore potential legal liability, between rights holders and the museum.

Another hurdle faced by the Brooklyn Museum's digitisation program is generating buy-in from other departments, staff, and administration within the Museum and educating them on the importance but not insurmountability of copyright law regarding digitisation. Wythe and her colleagues first educated themselves about copyright law and its effects on digitisation, synthesized this with the Museum's mission and goals, and explained the risks and benefits to other stakeholders within the Museum.[34] Collaboration with broader staff, including curators and public relations officers, was critical to proceed with the digitisation project; however, even once the broader staff understood and supported the project, it was still difficult to obtain the resources to implement the project. To these ends, Wythe relied heavily on interns to conduct the research to locate rights holders, send the non-exclusive licences and catalogue the replies in the museum's database.[35] Digital Collections also strategically selected works to digitise, focusing on artists with multiple works (which could be included in one licence), works currently on view in the galleries, artists who were easy to find and contact, and galleries that represent multiple artists.[36] The success of the museum's efforts is evident: almost 6000 works by over 400 artists with potential rights claims have been cleared in the last two years alone.[37] The museum's model of embracing copyright law while always remembering the overarching goal of accessibility will hopefully be replicated by other museums in the coming years, promoting digitisation around the world of works not in the public domain.

Museums' Use of Licensing Agreements for Works in the Public Domain[38]

In contrast to museums' relatively broad reading of copyright law and fair use in relation to the digitisation copyrighted works, many museums take a strict view of copyright law when it comes to digitising works for which they either hold the copyright or which are in the public domain. These museums frequently assert a copyright in the digitised reproduction of the works in their collection and require licensing agreements for third parties to use these images. These licensing agreements often impose even stricter terms of use than copyright law generally, restricting the re-use, and therefore greater access to, the digitised collection.[39]

Collaboration with broader staff, including curators and public relations officers, was critical to proceed with the digitisation project

28 *Id*.

29 *Id*.

30 Wythe (Boilerplate statements).

31 According to Wythe, this is the more frequent result than refusal. In returning the licence agreement, rights holders are permitted to grant some but not all of the rights that the Museum has requested. If the licence is entirely refused, the Museum continues to make the thumbnail available, relying on fair use of thumbnails analysed above. *See supra* note 25.

32 Wythe (Orphaned works worksheet).

33 The rights statement for orphan works reads as follows: "After diligent research, the museum is unable to locate contact information for the artist or artist's estate. We have therefore classified this work as 'orphaned.' If you have any information regarding this work and rights to it, please contact copyright@brooklynmuseum.org." Wythe (Boilerplate statements).

34 Wythe.

35 *Id*.

36 *Id.*

37 *Id*.

38 For more information on what works in a museum collection are likely in the public domain, *see* http://copyright.cornell.edu/resources/publicdomain.cfm

39 Crews, Kenneth D. and Melissa A. Brown, *Control of Museum Art Images: The Reach and Limits of Copyright and Licensing*. Prepared for the Proceedings of the Annual Congress of the International Association for the Advancement of Teaching and Research in Intellectual Property. Vilnius, Lithuania. 13-16 Sept 2009. At 6. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1542070. (Hereinafter "Crews").

many museums take a strict view of copyright law when it comes to digitising works for which they either hold the copyright or which are in the public domain

Copyright claims over digitised images of collection works are not as clear-cut as the museums which rely on these licensing schemes may wish. In order to claim a copyright under American law, the copyrighted work must be an "original work," requiring a minimum level of creativity in the conception and production of the work.[40] Since digitisation aims to accurately replicate the underlying work, courts have found that these images contain no "spark of originality" and are therefore not copyrightable.[41] While photographers and museums may oppose this, courts have been adamant that creativity, not the hard work, cost, and expertise required for digitisation, is the essential element protected by copyright law.[42]

In response to *Bridgeman* and similar cases, some museums have asserted that digital images of collection objects "depict…[the objects] in a manner expressing the scholarly and aesthetic view of the [museum]…and are protected by copyright."[43] These museums require those wishing to use these digital images, including scholars and academic publications, to sign a licensing agreement and pay licensing fees.[44] Once the third party has signed this licence agreement, they are bound, under contract rather than copyright law, to its terms. Most of these licences are highly restrictive, granting permission for only the specific use applied for at that time.[45] These licences restrict even such reproduction and use that would fall under the fair use exception in copyright law, including educational uses. Museums that use such restrictive licences justify these actions on two grounds: first, that as "stewards" of their collections, they have an obligation to ensure that these works are not misused or misrepresented, and, second, that making these digital images freely available would cut off a much needed revenue flow in the form of licensing fees which can also serve as a return on investment for the resources spent in digitisation.[46]

While both of these rationales seem valid on their face, the overall result of these licensing schemes (that is, the restriction of access to artworks in the public domain) stands in complete opposition to museums' educational goals – namely, the access to art for all. Backlash to these agreements has led several major institutions in recent years to make their collections more readily available online, even for third-party use; examples include the Brooklyn Museum's Creative Commons licence for public domain works, the Metropolitan Museum of Art's Images for Academic Publishing initiative which offers free, high resolution images from its collection for free to academics, and the Smithsonian which has added its public domain photography collections to the Flickr Commons.[47] By treating objects in their collection in the public domain as a public good that is widely available and non-exclusive, these institutions have embraced the values of access and public service.[48] Further, by expanding the reach of their collections online, these museums' educational missions continue even beyond the museums' walls.

Moving beyond digitising collections: Museum 2.0?

Some museums have, through online projects and in-gallery activities, taken digitisation a step further by seeking to redefine the museum experience as rooted in Web 2.0 values, norms and, practices.

After completing the digitisation of their collections, many museums struggle to encourage visitors to actually use these collection databases in a way that is engaging and relevant. Alongside the general digitisation trend, in recent years, a number of major museums have also relaunched their entire websites.[49] Among these relaunches, the Whitney Museum of American Art's stands out for its distinctly Web 2.0 approach, found in the methods used to create and distribute content and the offering of personal accounts which allow users to create their own "dashboards" of digital images and pages. The entire site was redesigned on a wiki platform so that all levels of museum staff would be able to contribute content while keeping a visually consistent site and brand identity.[50] In addition to staff, other stakeholders were also invited to contribute, including 55 artists participating in the 2010 Whitney Biennial, who could create their own individual pages in order to "create a direct relationship between the museum, the artists, and the public." This decentralized, wiki-based process was at first difficult for some internal stakeholders to accept; however, this emphasis on collaboration and interaction between departments has led to a website that staff feels is truly "a part of the Whitney – not just about the Whitney."[51]

The Whitney's website is also one of the first individual museum sites to allow site visitors to create a personal profile;[52] that is, a dashboard on which to collect images from the collection, upcoming

courts have been adamant that creativity, not the hard work, cost, and expertise required for digitisation, is the essential element protected by copyright law

40 Copyright Act of 1976 §101, 17 U.S.C. §102(a) (2010). *See also* Crews at 6-7.

41 *Bridgeman Art Library, Ltd. V. Corel Corp.*, 36 F.Supp2d 191, 197 (S.D.N.Y. 1999); *See also Meshwerks, Inc. v. Toyota Motor Sales U.S.A., Inc.*, 528 F.3d 1258.; Crews at 7-9.

42 *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 355, 359-60 (1991).; Crews at 9.

43 Museum of Fine Arts Boston, Terms and Conditions of Image Usage (2009). Available at http://www.mfa.org//master/sub.asp?key=45?key=2179. From Crews at 10.

44 Crews at 11.

45 *Id*. at 11-12.

46 *Id*. at 16.

47 *Id.* at 18

48 Daphna Lewinsohn-Zamir, *The "Conservation Game:" The Possibility of Voluntary Cooperation in Preserving Building of Cultural Importance*," 20 Harv. J.L. & Pub. Pol'y 733, 746-748 (1997)

49 Helal, D. et al., Barn Raising: Building a Museum Web Site Using Custom Wiki Tools. In J. Trant and D. Bearman (eds). *Museums and the Web 2010: Proceedings*. Toronto: Archives & Museum Informatics. Published March 31, 2010. Consulted April 21, 2011. Available at http://www.archimuse.com/mw2010/papers/helal/helal.html (Hereinafter "Helal").

50 Helal.

51 *Id.*

52 Other collaborative and regional sites have been created which allow users to create accounts and curate digitised collections. One such example of this is mainememory.net which allows schoolchildren to create their own narratives by piecing together digitised historical collections and then publish them online.

events, artist profiles, and other pages on whitney.org that appeal to them specifically. While there are many benefits to the user and the museum in building its own content platform, there are still some shortcomings to this system. There appears to be little opportunity for interaction or to view other users dashboards. Privacy is likely a key concern here, and the museum sensibly requires a minimal amount of information from those who register (only email address, password and zip code). In order to move the site to the next level, however, the Whitney must expand from a two way "dialogue" between one user and the museum, to a multidirectional dialogue which allows users to view others' dashboards in order to expand their own, communicate opinions and preferences, and start to form a true online community. This approach would enable museum sites like the Whitney's to find a niche that other Web 2.0 platform providers do not currently occupy. One possible niche has been described in general terms by Edson, who headed the Smithsonian New Media and Smithsonian 2.0 process: "Web magic truly happens when collections (or research data), experts, and the public are in close proximity."[53] Thus, the ideal platform that would synthesize this "close proximity" between the digitised collections, museum professionals and visitors, is yet to be seen.

Web 2.0 technology has also enabled new partnerships to develop, which provide the infrastructure and support for digitisation itself and then share the fruits of that labour. Institutions have been able to move beyond their internal limitations in resources, including holes in collections, underfunding and lack of technical expertise, to create museum platforms which are greater than the sum of their parts. One such example is Fluid Engage, a suite of museum-specific technology developed by an open source community of museums, galleries, designers and developers.[54] By working in an open-source community, this project enabled contributors from institutions as diverse as the Detroit Institute of Arts, the McCord Museum of Canadian History and the Museum of the Moving Image to develop low-cost and highly flexible interactive platforms for use in galleries, online, and on third-party devices like cell phones. These institutions were able to contribute to and receive software which was already integrated with existing collections management systems and software at each institution and which was open-ended enough to fit each institutions' highly individual goals. By designing their own software through collaborative wikis instead of relying on closed, commercial software, these designers and museum administrators tapped into the creative, community-driven power of Web 2.0 platforms to create a solution, founded on "openness…configurability, and flexibility," to solve each of their individual needs.[55]

Moving beyond technologies in the galleries, could museum exhibition design and communication more fully embrace the underlying values – creativity, collaboration, and exchange – of the Web 2.0 experience? Nina Simon, a writer, museum consultant and now museum director, has challenged museums to use Web 2.0 not simply as a technological tool to encourage engagement but as an overarching model to redesign the galleries as a forum where even complete strangers have the opportunity for "interpersonal discourse."[56] Simon's conception of Museum 2.0 is inherently social, supports "diverse access paths" to content, objects, and experiences, and is democratic, developed and accessed from the bottom-up.[57] Many museums, including those examined here like the Brooklyn Museum and the Whitney, have aggressively pursued Simons' strategies for Web 2.0 online activities such as creating blogs, collection databases, podcasts, iPhone apps, and Facebook pages; few, however, have taken the more revolutionary step of integrating the principles of sociality, accessibility, and democracy into the real world galleries.

At the San Diego Museum of Natural History during a gallery reinstallation, the exhibit team implemented a program called "Case by Case." In the gallery, objects from the collection were on display without any didactics (traditionally, explanatory text on labels alongside the object), and visitors were invited to literally "tag" the objects on display with questions or observations they had on post-its.[58] From this, curators and designers were able to discover questions they never would have thought of otherwise. Didactics were then crafted to answer visitors' questions and placed alongside the objects. Even the questions themselves became part of the exhibition and the learning experience as designers decided to display them alongside the completed, traditional explanatory label.[59]

"Case by Case" demonstrates a new way to engage visitors with objects, exhibitions, and the museum as a whole. Visitors have the opportunity to approach the museum through the lens of their own experiences, contribute their viewpoint to the newly multi-vocal and bottom-up museum, and feel that their views are valued, addressed, and incorporated into the exhibit which allows the creative process to start anew with the next visitor. These approaches are limited by the difficulty of, what Simon describes as, moving from interaction between "me" and the museum and "we in the museum."[60] Only by building a communal, social space founded on respect, exchange, and collaboration can museum exhibits become spaces for "collective social interaction."[61]

Conclusion: Museum 2.0 is only the beginning

As museums continue to find new ways to increase access to their collections through digitisation, to navigate potential legal liabilities as they bring their collections into the 21st century, and to engage continuing and new visitors both in the galleries and online, Web 2.0 can serve as a model for how to approach these complexities in an open, social, and collaborative framework. However, Web 2.0 principles integrated into the Museum 2.0 proposed by Simon can only take us so far. New initiatives like Google Art Project bring ever more complexities to the table: how, and to what extent, should museums as public organizations work with private corporations to digitise and share their collections? What role should consortiums and collaborations play in the future of museums, and who is responsible for their success or failure? In order to meet these ever-emerging challenges, museums must embrace the hybrid values examined in the first part of this paper: accessible authenticity and flexible conservation. By merging the traditional values that work for museums, which have empowered them for centuries to create authentic cultural experiences, and emerging values of digital natives, museums can remain relevant and engaging homes of science, history, art, and culture for generations to come.

Susan Sheffler has an MA in Museum Studies from New York University, and is currently a JD candidate at Harvard Law School.

---

53 Edson.

54 Mitchell, J. et al., New Technology in the Museum: A Case Study of Three Museums in the Fluid Community Working Together. In J. Trant and D. Bearman (eds). *Museums and the Web 2010: Proceedings*. Toronto: Archives & Museum Informatics. Published March 31, 2010. Consulted April 21, 2011. Available at http://www.archimuse.com/mw2010/papers/mitchell/mitchell.html.

55 *Id*.

56 Simon at 258.

57 *Id*. at 259.

58 Blackford, Kim, et. al. *Guest Post: Using Visitor Participation to improve Object Labels at the San Diego Natural History Museum*, Museum 2.0, 29 March 2011.

59 *Id.*

60 Simon at 267.

61 *Id.*

Personal Privacy Protection in Australia: A Statutory Solution

Henry Fraser and Rowan Platt examine the proposal made by the ALRC and recently addressed in the Government's Issues Paper for the introduction of a statutory cause of action for invasion of privacy.

The Federal Government is currently consulting on whether it should legislate to protect personal privacy by creating a statutory cause of action that will allow individuals to sue for serious invasions of privacy. The Government's September 2011 Issues Paper[1] follows the Australian Law Reform Commission's 2008 recommendation[2] for the introduction of a statutory cause of action. It also refers to similar proposals since made by the New South Wales[3] and Victorian Law Reform Commissions.[4] The Government's Issues Paper discusses whether there is ultimately a need for a statutory cause of action for serious invasion of privacy; and if so, what elements it might consist of, and what defences and remedies should be made available. Whilst the final form any legislation might take is not yet known, such a cause of action would provide certainty about what type of invasive conduct, and what type of harm would give rise to liability for a serious invasion of privacy.

This article briefly examines the existing privacy law landscape in Australia, before assessing the merits and potential difficulties faced by the current proposal, such as whether the proposed cause of action strikes the right balance between an individual's interest in privacy and the public interest in freedom of the press.

The modern privacy context

In 1937 the High Court considered whether a racetrack owner was entitled to prevent a broadcaster from calling the races from a platform constructed on the adjacent property.[5] In determining whether there was a legal basis for preventing the invasion of the owner's privacy, Chief Justice Latham suggested that "[i]f the plaintiff desires to prevent [people looking over his fence], the plaintiff can erect a higher fence".[6] For a long time, the case stood for the proposition that there is no right to personal privacy in Australia.

Over the past ten years, however, courts have begun to reconsider whether invasions of privacy may be compensable. One factor that has heightened the risk of invasion of privacy during this time is the development in mobile and internet technology. A smart phone's audio, picture and film recording functions allow people to take and share content without the knowledge of the subject. The name given to this emerging trend is a metaphor for the speed with which the information is disseminated across networks - "going viral". The content is typically stored on social networking sites. Like most other cloud based software, user data is stored on a remote server that is vulnerable to hacking. Even without hacking, the terms and conditions of such websites may permit the service provider to deal with personal information in a way that users did not expect. In either of these ways, personal content can be mined for either commercial or more sinister purposes.

Recently data and security breaches have received increasing media attention. Hackers are achieving a level of notoriety and fame. The risks of data and security breaches are likely to increasingly affect individuals as more personal information is moved to 'the Cloud'. There have also been egregious breaches of personal privacy that have recently come to light during the News of the World inquiry. Protecting individual privacy in the 21st century has become substantially more difficult than simply erecting a higher fence.

The risks of data and security breaches are likely to increasingly affect individuals as more personal information is moved to 'the Cloud'

Nonetheless, seventy four years after the *Victoria Park Racing* case, there is still no right to personal privacy in Australia. Under the *Privacy Act 1988* (Cth), protection is focussed on the collection, use and distribution of personal information, rather than on invasion of privacy generally. All enforcement is left in the hands of the Privacy Commissioner: individuals have no power to take independent legal action for infringements. The position in analogous State and Territory Legislation is similar.[7]

Before considering the proposed statutory cause of action for invasion of privacy, it is instructive to note how the Australian courts have dealt with cases involving breaches of privacy. In particular it is interesting to observe how the different circumstances confronting the courts have shaped some of the elements comprising the proposed statutory cause of action.

Common law tort of privacy

In 2001 the High Court in *ABC v Lenah Game Meats*[8] removed what was considered to be the major obstacle[9] to the recognition of a

1 *A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy*, September 2011

2 'For Your Information: Australian Privacy Law and Practice', *ALRC Report 108*, 11 August 2008

3 New South Wales Law Reform Commission, *Report 120: Invasion of Privacy* (2009) (NSWLRC Report) available at <www.lawlink.nsw.gov.au/lawlink/lrc/ll_lrc.nsf/vwFiles/R120.pdf/$file/R120.pdf>.

4 Victorian Law Reform Commission, *Surveillance in Public Places: Final Report 18* (2010), ch 7 (VLRC Report) available at <www.lawreform.vic.gov.au/wps/wcm/connect/justlib/Law+Reform/Home/Completed+Projects/Surveillance+in+Public+Places/>.

5 *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479

6 Ibid, at 494

7 See, for example, the *Privacy and Personal Information Protection Act* 1998 (NSW) under which the Privacy Commissioner is required to resolve any 'privacy related complaint' by arbitration

8 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd('Lenah Game Meats')* (2001) 208 CLR 199, at 248.

9 For further discussion on this point, see D Butler, 'Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339, 341; and Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy,* ALRC 11 (1979), [223].

Under the Privacy Act 1988 (Cth), protection is focussed on the collection, use and distribution of personal information, rather than on invasion of privacy generally. All enforcement is left in the hands of the Privacy Commissioner: individuals have no power to take independent legal action for infringements.

common law right to privacy in Australia, by clearly indicating that its 1937 decision in *Victoria Park Racing*[10] no longer stood in the path of a cause of action developing. The court did not, however, make the leap to recognising that a tort of privacy exists. Indeed, as the New Zealand Court of Appeal later observed, 'the High Court of Australia has not ruled out the possibility of a common law tort of privacy, nor has it embraced it with open arms'.[11] Since *Lenah Game Meats*, two lower courts have held defendants liable in tort for invasion of privacy, but no appellate court has confirmed that the tort is now a valid cause of action.[12]

In the Queensland District Court decision of *Grosse v Purvis*, Senior Judge Skoien held that a case of persistent stalking amounted to an invasion of privacy. He formulated the elements of a fledgling tort as including: (i) a willed act by the defendant; (ii) which intrudes upon the privacy or seclusion of the plaintiff; (iii) in a manner which would be considered highly offensive to a reasonable person of ordinary sensibilities; and (iv) which causes the plaintiff detriment in the form of mental, psychological or emotional harm or distress or which prevents or hinders the plaintiff from doing an act which he or she is lawfully entitled to do.[13] His Honour also noted that a public interest defence should be made available.[14]

In *Doe v Australian Broadcasting Corporation*, in the County Court of Victoria, Judge Hampel held that the publication of the identity of a rape victim was, inter alia, a tortious invasion of privacy. Responding to the suggestion that recognition of a tort of privacy would be a 'bold step', her Honour asserted that the cases 'decided since *Lenah Game Meats* demonstrate a rapidly growing trend towards recognition of privacy as a right in itself deserving of protection'.[15] While she did not formulate a precise description of the elements of a cause of action, she did note that the wrong included 'the publication of personal information, in circumstances where there was no public interest in publishing it'.[16]

Despite the recognitions made in these two cases, appellate courts have cited two main obstacles to the tort's development: the lack of precision in the concept of privacy, and the difficulty of balancing the interest in personal privacy with the interest in free speech and publication.[17]

Breach of confidence – extension to private information

Although a common law tort of invasion of privacy has not yet developed, the equitable action for breach of confidence has expanded to furnish a degree of protection for personal privacy. Since *Lenah Game Meats*, Australian courts have accepted that a duty of confidence may arise from circumstances rather than exclusively from a relationship of trust and confidence.[18] In that case Gleeson CJ identified three elements required to prove a breach of confidence: (i) that the information is confidential; (ii) that it was originally imparted in circumstances importing an obligation of confidence; and (iii) that there has been, or is threatened, an unauthorised use of the information to the detriment of the party communicating it.[19] His Honour suggested that private information could satisfy the first two requirements and formulated as a practical test of what is private, "the requirement that disclosure or observation of information or conduct would be highly offensive to a reasonable person of ordinary sensibilities".[20] Gleeson CJ's test of what is private was endorsed by Judge Skoein in *Grosse v Purvis*, in characterising invasion of privacy as a tort rather than merely another form of breach of confidence, and subsequently, by the ALRC, NSWLRC and VLRC in their respective reports.

In *Doe*, Judge Hampel added to Gleeson CJ's test a formulation of privacy from the UK case of *Campbell v MGM Ltd.*[21] Her Honour defined private or confidential information as information in respect of which a person has a reasonable expectation of privacy. Whether there is a reasonable expectation of privacy will be a matter for evidence from case to case. So even information which has some degree of public exposure may sometimes be considered private or confidential. The upshot of *Lenah Game Meats* and *Doe* is that circumstances which give rise to a reasonable expectation of privacy are also capable of giving rise to a duty of confidentiality. The concept of a reasonable expectation of privacy also features in the elements of the ALRC's proposed statutory cause of action.

In the Victorian Court of Appeal decision of *Giller v Procopets*, the court considered a claim brought in the context of a former de facto relationship where the defendant had published (to the plaintiff's

Although a common law tort of invasion of privacy has not yet developed, the equitable action for breach of confidence has expanded to furnish a degree of protection for personal privacy

10 *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479

11 *Hosking v Runting* [2005] 1 NZLR 1, at [59] per Gault P and Blanchard J. See also G Taylor and D Wright, 'Australian Broadcasting Corporation v Lenah Game Meats: Privacy, Injunctions and Possums: An Analysis of the Court's Decision' (2002) 26 *Melbourne University Law Review* 707, 709.

12 *Grosse v Purvis* [2003] QDC 151; *Kalaba v Commonwealth of Australia* [2004] FCAFC 326; *Doe v Australian Broadcasting Corporation ('Doe')* [2007] VCC 281; *Giller v Procopets* [2008] VSCA 236

13 *Grosse v Purvis* [2003] QDC 151 at [444].

14 Ibid, at [34].

15 *Doe v Australian Broadcasting Corporation* [2007] VCC 281, at [161].

16 Ibid, at [163].

17 *ABC v Lenah Game Meats* (2002) 208 CLR 199 at 41 and 225; *Giller v Procopets* [2008] VSCA 236 at [167] – [168] per Ashley JA and [447-452] per Neave JA.

18 *Lenah Game Meats* at [34], see also *Doe* at 112.

19 *Lenah Game Meats* at [30].

20 *Lenah Game Meats* at [40].

21 [2004] 2 AC 457 at [13]-14].

The Government's recent Issues Paper on the proposed 'Commonwealth statutory cause of action for serious invasion of privacy', draws principally on the ALRC recommendations

friends and family) a video he had filmed of his sexual activities with the plaintiff, some with the plaintiff's consent. The court found that this was a breach of confidence and awarded the plaintiff damages for her mental distress.[22] All three judges noted that while the common law does not provide a remedy for mere distress, equity could provide relief for embarrassment, humiliation or distress.[23]

Despite the recent success of plaintiffs protecting their private information by pleading breaches of confidence, the action into which the protection of privacy is now 'shoe-horned'[24] in English law, there is an important limitation on the use of breach of confidence to address privacy issues. The action is confined to cases involving the *use* of private information. There will be no cause of action for breach of confidence until an intrusive photograph or private information is published.[25] This means that using the equitable action to protect privacy would protect against the conduct in cases like *Doe*, but would provide no cause of action to remedy equally invasive and harassing conduct where there is no actual publication, such as the stalking that took place in *Grosse v Purvis.*

The answer?: the creation of a statutory tort

In its 2008 report,[26] the ALRC asserted that the enactment of a statutory cause of action for invasion of privacy would both provide broader protection than the equitable action for breach of confidence, and offer more certainty than the unestablished common law tort. In its submission for the ALRC consultation process, the Commonwealth Office of the Privacy Commissioner argued that 'a dedicated privacy based cause of action could serve to complement the existing legislative based protections afforded to individuals and address some gaps that exist both in the common law and legislation'.[27] It would also alleviate the need for judges to refine the standard and elements of the cause of action on a case-by-case basis. This would provide certainty as to the defences and remedies available, as the distinction between equitable and tortious causes of action would be removed.

The Government's recent Issues Paper on the proposed 'Commonwealth statutory cause of action for serious invasion of privacy', draws principally on the ALRC recommendations. The following is an assessment of the proposed cause of action and its principal features, some of which have already been subject to heated debate in the press.

The proposed statutory tort

Elements

Under the ALRC's proposal, in order to establish the cause of action for serious invasion of privacy, a claimant would need to show that, in all the circumstances:

- they had a reasonable expectation of privacy;
- the defendant's act or conduct was highly offensive to a reasonable person of ordinary sensibilities; and
- the public interest in maintaining the claimant's privacy outweighs other matters of public interest, (including the public interest in allowing freedom of expression and the interest of the public to be informed about matters of public concern).

The first thing to note is the objective test of seriousness. The adoption of the 'highly offensive' formulation from *Lenah Game Meats* is intended to set a high threshold, narrowing the range of circumstances in which a plaintiff could successfully demonstrate a serious invasion of privacy. The advantage of this formula is that the courts will already have some guidance as to its application from the cases discussed above, and from New Zealand cases.[28]

Recognising Freedom of Expression: A Balancing Test

Perhaps more significant and controversial is the manner of weighing the public interest that the ALRC has proposed. Rather than attempting to protect other public interests like freedom of expression through a defence such as fair comment (as was proposed in its earlier report[29] and by the VLRC), the ALRC took the view that it would be better in both principle and practice to add an additional element to the cause of action. The inclusion of such a balancing test would ensure that individual privacy rights are not privileged over other public interests. It would achieve this by placing on the claimant the burden of demonstrating that an invasion of privacy was not in the public interest. Rather than defendants, such as media organisations, being required to demonstrate, for example, that the publication of private material was in the public interest, the claimant would be required to prove that the contrary was true. This would also help to guard against unmeritorious claims, and would set a higher threshold for what could be considered a serious invasion of privacy. An invasion of privacy would only be unlawful if it were not in the public interest. Accordingly, bona fide investigative journalism about matters of pubic interest would presumably be unlikely to attract liability.

Whether the public interest in freedom of expression might be better protected or recognised in some other way will undoubtedly be the subject of many submissions from media organisations.

No need to prove harm

As with the torts of defamation and trespass to the person, the cause of action of invasion of privacy would be actionable *per se*: without any requirement that the claimant prove that any actual damage or calculable loss was suffered as a result of the invasion of privacy. This would neutralise the debate over whether causing mere distress, as opposed to psychological or economic harm, would incur liability.

In the ALRC's view it is important that the cause of action not be used as an intellectual property style personality right to protect commercial value

---

22 *Giller v Procopets* [2008] VSCA 236 at [159] per Ashley JA and [423] per Neave JA.

23 *Giller v Procopets* [2008] VSCA 236 at [159] per Ashley JA and [423] per Neave JA.

24 *Douglas v Hello! Ltd (No 3)* [2006] QB 125, [53].

25 Sir R Toulson, 'Freedom of Expression and Privacy' (Paper presented at the Association of Law Teachers Lord Upjohn Lecture, London, 9 February 2007), 7.

26 In *ALRC Report 108*, the ALRC handed down nearly 300 recommendations on reform of Australian privacy law and practice, one of which was the introduction of a statutory cause of action for invasion of privacy.

27 Office of the Privacy Commissioner, *Submission PR 499* [to the ALRC Privacy Review], 20 December 2007.

28 *Hosking v Runting* [2005] 1 NZLR 1, at [117].

29 Australian Law Reform Commission, *Review of Australian Privacy Law,* DP 72 (2007), Proposal 5-5.

there is no proposed exemption for media organisations that publish sensitive information about an individual's private life

The requisite fault element

The ALRC recommended that the cause of action for serious invasion of privacy be restricted to intentional or reckless acts by the respondent. Recklessness, which is defined in Section 5.4 of the *Criminal Code Act 1995* (Cth), occurs where a person is aware of a substantial risk that a circumstance or result will occur, but continues in their conduct notwithstanding their knowledge of that risk. The Issues Paper explains that this would preclude actions brought where there has been only a negligent or accidental invasion of privacy.[30]

By comparison, the standard required of corporations under National Privacy Principle 4 of the *Privacy Act* is to take 'reasonable steps' to protect against information privacy breaches. Arguably, the proposed fault element of recklessness will make it more difficult to impose liability on corporates for data breaches, as it will require evidence of their knowledge of a risk or a situation where they ought to have known about the risk which has eventuated.

What type of acts or conduct will it protect against ?

The ALRC's recommendations recognise that individuals should be protected from unwanted intrusions into their private lives or affairs in a broad range of circumstances, irrespective of whether the act or activity takes place in private. To that end, it was proposed that the legislation contain a non-exhaustive guiding list of the types of activities and conduct that may constitute serious invasions of privacy, including:

(a) a serious interference with an individual's home or family life;

(b) unauthorised surveillance of an individual;

(c) interference with, or misuse or disclosure of, an individual's correspondence or private written, oral or electronic communication; and

(d) disclosure of sensitive facts relating to an individual's private life.

The ALRC considered that such a list would alleviate the need for judges to define the notion of serious invasions of privacy by construing the statute and its words over time against evolving notions of privacy.

In the ALRC's view it is important that the cause of action not be used as an intellectual property style personality right to protect commercial value (as, for example, was the case in the UK case of *Douglas v Hello!*). Under the proposed cause of action, exploitation of a person's identity or likeness without their consent that damages the person's reputation would not be characterised as an invasion of privacy.

The Issues Paper asks whether a non-exhaustive list of activities should be included in the legislation itself or in the other explanatory material.

Defences and Exemptions

The ALRC proposed that a range of defences to the cause of action should be available where:

- the act or conduct was incidental to the exercise of a lawful right of defence of person or property;
- the act or conduct was required or authorised by or under law; or
- the publication of the information was privileged under defamation law.

The ALRC recognised that any cause of action should not impede legitimate law enforcement and intelligence activities but did not recommend a blanket exemption for particular types of organisations or agencies. The Issues Paper asks whether these are appropriate and whether particular types of organisations should be excluded from the ambit of the proposed cause of action, or whether defences should be used to restrict its application.

Remedies

The ALRC recommended that the court, if satisfied that a serious invasion of privacy has been established, should be empowered to choose the most appropriate remedy in the circumstances, including damages, aggravated (but not exemplary) damages, an accounts of profits, an injunction, declarations, a court-ordered apology, correction orders and an order to deliver up and/or destroy material. The Issues Paper asks whether these remedies are necessary and sufficient. It also asks whether it is desirable to include an appropriately adapted offer-of-amends process, similar to that which was created by recent reforms to the law of defamation.[31]

Class actions

The Issues Paper also briefly discusses the possibility of claimants bringing class actions for serious invasions of privacy where claims arise out of similar or related circumstances. Providing that the claim gave rise to a substantial common issue of law or fact,[32] class action rules could have application in claims where an individual or company's act resulted in a serious invasion of privacy.

Who will be affected?

Whatever the precise formulation, it can reasonably be expected that the introduction of any separate statutory cause of action for invasion of privacy will require a range of businesses to reassess their privacy practices to minimise their liability.

Importantly, despite the ALRC's suggestion that the proposed cause of action should not hinder legitimate investigative journalism (that deals with, for example, allegations of misconduct or corruption in public life, and other matters of genuine public concern), there is no proposed exemption for media organisations that publish sensitive information about an individual's private life. This would be an important departure from the current position under the *Privacy Act*, where media organisations are afforded an automatic exemption from compliance with the Act where they use personal information in the course of journalism.[33] Nonetheless, the formulation of the balancing test as an element of the cause of action is calculated to favour freedom of the press over privacy plaintiffs, in circumstances where publication of private material is in the public interest.

The Issues Paper makes clear that the Government is desirous of strengthening our privacy law, but not at the expense of freedom of expression and the freedom of the media to seek out and disseminate information of public concern.

Henry Fraser and Rowan Platt are lawyers in the Technology, Media and Telecommunications Practice Group at Allens Arthur Robinson.

30 See NSWLRC, *Invasion of Privacy*, Consultation Paper 1(2007) at [7.24] for the view that including accidental or negligent acts 'would, arguably, go too far'.

31 Now found in ss 12-19 Uniform Defamation Laws

32 See s 33C(1) *Federal Court Act 1976* (Cth) for requirements that apply to 'representative proceedings'.

33 *Privacy Act 1988* (Cth), section 7B(4).

Challenges and Choices: Universal Service in Australia and China

Thomas Jones and Sarah Godden examine the similar challenges faced by Australia and China in the provision of universal telecommunications services to remote areas and the opportunities for knowledge sharing and co-operation between the two countries.

Much has been written about the differences between China and Australia but far less about the similarities. Yet the two countries face similar challenges in the provision of universal telecommunications services - challenges which provide an opportunity for co-operation and knowledge sharing.

While China's population density of 143 people per square kilometre significantly exceeds Australia's, much of its population, like our own, is concentrated along the densely populated east coast with significant tracts of sparsely populated inland areas. It is these areas which pose the greatest challenge in providing cost effective telecommunications services.

Why provide universal service?

There are cogent social, political and economic arguments made in support of the provision of universal service.[1] Increasingly, these arguments are being advanced to the stage where access to telecommunications services is recognised as a virtual human right. For example, the May 2011 report from the Human Rights Council of the United Nations General Assembly declared access to the Internet a basic human right which enables individuals to 'exercise their right to freedom of opinion and expression.'[2] Several European nations, including Estonia, Finland, France, Greece and Spain, have passed domestic legislation recognising citizen's right to access the internet. Some of these countries have even codified minimum speeds (Finland, Spain).

There is a corresponding rise in the view that internet services (and in developed countries, even broadband services) should be considered part of any universal service obligation.[3] If so, what level of service is required? How do these investment decisions interact with the investment required to provide universal telephony services in regions which do not yet have access to either service? Could both services be provided using wireless technology? If these services can be provided comparatively quickly and efficiently using wireless, do these considerations outweigh quality of service concerns?[4]

Universal service in Australia

In Australia, the Government has recently changed its approach to this challenge by establishing NBN Co and moving to a contractual model for universal service delivery. China is rolling out universal services to its population, focussing on voice and broadband services. The common question for both is: what is the most equitable and efficient way to deliver these services?

Delivery of broadband services in Australia

NBN Co was established to build the $36 billion National Broadband Network, a key plank of the Australian Government's commitment to "...provide Australians with access to high quality broadband services, no matter where they live or work".[5] Construction of the network has commenced in discrete modules across Australia.[6] The Australian Government has committed to a uniform national wholesale price for the entry level wholesale broadband service designed for 12/1Mbps at the layer 2 level to be provided from 121 points of interconnect across Australia. Inevitably this means that some degree of subsidisation of high cost regional and rural services by lower cost metropolitan services will occur.

Changing the delivery of universal service in Australia

As the NBN has entered into agreements with Telstra for the provision of wholesale access to the NBN, the approach to universal service provision at the retail layer has also had to change. Currently Telstra, the fixed-line incumbent, is required to make voice services available to all on request. It generally fulfils these obligations by provision of services over its ubiquitous copper network.

However, once Telstra's copper network is decommissioned as part of its agreement with NBN Co (assuming the Australian Competition and Consumer Commission approves those arrangements[7]), it will no longer be appropriate to regulate Telstra as the 'carrier of last resort'. Instead the Australian Government has decided to move to a contractual model, which recognises that service providers will ultimately be able to provide voice and broadband services over the NBN.

As part of the reforms, a new Commonwealth agency, the Telecommunications Universal Service Management Agency (***TUSMA***) is being established to contract with retail service providers to provide universal service over the NBN. TUSMA will periodically tender for the provision of these services, enabling competition to emerge. However, given the complex issues with the transition to the NBN and the interrelationship with the arrangements between NBN Co and Telstra, the initial contract will be with Telstra. This structure also reflects the com-

---

1 Clarke GRG and Wallsten SJ, *Universal(ly Bad) Service: Providing Infrastructure Services to Rural and Poor Urban Consumers*, World Bank Policy Research Working Paper 2868, July 2002, pp5-10; Manner JA, *Achieving the Goal of Universal Access to Telecommunications Services Globally*, (2004) 13 Commlaw Conspectus 85 at 87; Cremer H, Gasmi F, Grimaud A and Laffont JJ, *Universal Service: An Economic Perspective*, (2001) 72 Annals of Public and Cooperative Economics 5 at 12-13, 18.

2 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17th session of the Human Rights Council of the United Nations General Assembly, 16 May 2011 http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (accessed 6 September 2011).

3 Shi J, *Telecommunications Universal Service in China: Making the Grade on a Harmonious Information Society*, (2008) 13 Journal of Technology Law & Policy, 115 at 128.

4 Particularly in regional areas where the distance from an exchange is likely to severely affect speeds of broadband services provided over copper line infrastructure.

5 Senator Conroy, *Australian Broadband Guarantee funding until 2012*, press release dated 13 May 2008, available: http://www.minister.dbcde.gov.au/media/media_releases/2008/032 (accessed 6 September 2011).

6 http://www.nbnco.com.au/our-network/rollout-plan.html (accessed 7 November 2011).

plex economic issues which arise in the provision of a fundamentally unprofitable service with significant positive externalities, such as universal service. Where the forces of normal market competition cannot be harnessed, economic literature suggests that periodic competition for the market (e.g. by way of periodic tender for a monopoly contract) could be a 'second best' option.[8]

Increasing competition may be one way of increasing penetration (where universal coverage has not been achieved) and service.[9]

Universal service in China

In China, the Government is aiming to ensure that all parts of the country benefit from development and technological change. The provision of universal telecommunication services is one way to achieve better outcomes in rural and remote areas. It also dovetails with the increasing tendency world wide to see access to telecommunication services as a virtual human right, discussed above.

The Twelfth Five Year Plan (2011-2015) outlines the Chinese Government's investment priorities: including in the areas of broadband networks, internet security infrastructure and network convergence.[10] Investment in broadband networks is planned to include promoting fibre to the home networks (FTTH) in urban areas, speeding up the construction of broadband networks in rural areas, improving broadband penetration and increasing bandwidth.[11] On the ground, China Telecom has announced plans to replace its copper network with fibre optic cable over this period.[12]

Considerations for investment

Both countries face challenges in identifying appropriate areas to target for their infrastructure investment, which must balance equity and efficiency concerns. Australia's NBN Co is treating rural and regional areas as a key focus in terms of timing of the rollout,[13] although metropolitan areas also feature in some of the first and second release sites. The Chinese Government's significant investment will benefit both urban and regional areas. In China, the focus in urban areas is on upgrading service quality, while in regional areas the challenge is still to improve household penetration rates.

Historically the Chinese Government's emphasis has been on providing universal access, rather than universal service (i.e. access to telephony services in each administrative village). With this objective now achieved, the focus naturally shifts to connecting natural or actual villages,[14] followed by households.[15] Due to the sheer size and scope of the task,[16] the Government of China faces enormous challenges in providing telephony services to its entire population. While 100% of administrative villages have voice telephony services as at 2010, taken on a household level fixed line services achieve only 22% penetration, clearly lagging mobile (voice) penetration of 64%.[17] Although these numbers are steadily increasing,[18] they indicate the massive investment which will be required to provide universal service to 1.3 billion citizens across 9.3 million square kilometres.

Under the twelfth five year plan, the total spend on broadband construction is planned to approximate RMB1.6 trillion (approximately $US251 billion) over the five years. This is reported to be an attempt by the Chinese Government to reverse a decline in take up of fixed line services, in favour of mobile services, in recent years.[19] This trend appears to be due as much to the higher levels of customer service available from mobile operators as to more favourable pricing.

This trend is indicative of another of the major challenges facing providers of universal service, choice of technology. Must universal service be provided by fixed line infrastructure? What level of service is required by a population? Is there sufficient value in the incremental service gains from fixed over wireless to justify the additional expenditure? Does the equation change once broadband services are considered in this mix? In Australia at least, the answer to this final question is yes.[20]

the Australian Government has decided to move to a contractual model, which recognises that service providers will ultimately be able to provide voice and broadband services over the NBN.

Choices and challenges

In China, as in Australia, there are challenges in providing universal service to citizens in rural and remote areas, irrespective of the model adopted. A key question for both countries is how to reach these areas efficiently. There are choices around selecting the right mix of technologies – fibre, copper, fixed and mobile wireless and satellite. There are also choices to be made about funding. For example, should high cost areas be explicitly subsidised by government or should the universal service provider subsidise these services with revenue obtained in lower cost areas? How can the forces of competition best be harnessed to promote efficiency in the provision of a fundamentally unprofitable service? Should both supply (investment) and demand (price) be supported or can the latter be left to market forces if there is competition on the supply side?

These questions can be contentious as they involve balancing economic efficiency and equity considerations. However, the prize for both nations, in terms of enhanced social welfare (in the total economic sense), is considerable. Arguably, the enormous productive capacity of China and its ability to shape events on the world stage will be significantly enhanced by universal access to telecommunications services. Similarly , universal access to telecommunications services is a key element of Australian social policy and, for many years, has been a critical means by which the 'tyranny of distance' has been overcome.

Thomas Jones is a partner and Sarah Godden is a senior associate at Corrs Chambers Westgarth.

---

7 The migration of services from the Telstra network to the NBN form part of a structural separation undertaking currently being considered by the ACCC.

8 *Re Sydney Airports Corporation Ltd* (2000) 156 FLR 10 at [113] – [115]; *Stirling Harbour Services Pty Ltd v Bunbury Port Authority* [2000] FCA 1381 at [21], [24].

9 Clarke GRG and Wallsten SJ, above n. 1 , pp 32-35.

10 BuddeComm, *China – Key Statistics, Telecom Market, Regulatory Overview and Forecasts.*

11 Ibid.

12 http://www.china.org.cn/business/2011-02/17/content_21943188.htm (accessed 27 October 2011).

13 A partial reason for this is the deal struck between the minority Government and two key independents. See clause 3.1, Annexure B, '*Agreement between The Australian Labour Part & the Independent Members (Mr Tony Windsor and Mr Rob Oakeshott)*', 7 September 2010. Available: http://www.alp.org.au/federal-government/government-agreements/ (accessed 27 October 2011). This is largely reflected in NBN Co's current 12 month roll out plan: http://www.nbnco.com.au/news-and-events/news/nbn-co-releases-12-month-national-rollout-plan.html

14 As distinct from the administrative village, which is a government designation similar in concept to an Australian municipal council.

15 Above n. 3 at 122-123.

16 For example, Shi states that in 2005, there were 732,700 administrative villages containing 5 million physical villages and 210 million households: Above n. 3 at 122.

17 Above n.10.

18 Above n.3 at 117.

19 Above n. 10, http://www.businesswire.com/news/home/20110706005057/en/Research-Markets-China---Key-Statistics-Telecom (accessed 27 October 2011).

20 The NBN fibre optic network will cover 93% of addressable premises, with the remaining 7% being covered by either fixed wireless or satellite technology. In this final 7%, premises will not be disconnected from the copper network and telephone services will continue to be available.

Consumer Protection Enhancements for the Australian Telecommunications Industry

Shane Barber reviews the work of both Communications Alliance and the ACMA in 2011 as they seek to address the Australian telecommunications consumer protection regime

The telecommunications industry, its regulators and its consumers have spent much of 2011 analysing, debating and reforming the Australian telecommunications consumer protection environment. The result is the publication of two influential works, being:

1. The Australian Communications and Media Authority's (***ACMA***) final *Reconnecting the Customer* report, published on 9 September 2011 (*Reconnecting the Customer*); and
2. Communications Alliance Limited's (***Communications Alliance***) draft *Telecommunications Consumer Protections Code 2011* released for public comment on 25 October 2011 (***2011 Code***).

For instance, the ACMA may prepare its own standard if it is satisfied that an industry code is deficient and that deficiency is not addressed by the industry prior to the end of a remedy period

Both works have been the subject of considerable consultation undertaken throughout 2010 and 2011 and are published after a year in which much media analysis was made of the telecommunications industry's performance in relation to the consumer experience. Both also come in the wake of the implementation of the new *Competition and Consumer Act 2010* (Cth) (***CCA***).

While both documents point to considerable reforms in store for the industry in 2012, a closer analysis of the documents reveals that both the regulator and industry have finished the year with substantially similar outcomes, with the variances being largely one of degree.

Telecommunications Consumer Protection Code

Background

Under the telecommunications industry's self regulatory environment, established by the *Telecommunications Act 1997* (Cth) (***Act***), bodies representing sections of the telecommunications industry are encouraged to develop industry codes. Communications Alliance, variously named, was formed in 1997 to fulfil that role for industry participants.

Pursuant to the Act, Communications Alliance may submit its various draft codes to the ACMA for registration and once registered, the ACMA may take enforcement action against industry participants who do not comply with them.

Importantly, the ACMA is not obliged to register codes proffered by the industry and, in some circumstances, may make its own industry standards which will apply to industry conduct in place of or in addition to codes prepared by the industry. For instance, the ACMA may prepare its own standard if it is satisfied that an industry code is deficient and that deficiency is not addressed by the industry prior to the end of a remedy period.

Back in 2007, Communications Alliance published and registered its initial *Telecommunications Consumer Protections Code 2007* (***2007 Code***), being a consolidation of a number of more specific codes published prior to that time. The 2007 Code was scheduled for a review in 2010/2011, a time which coincided with heightened community expectations of telecommunications industry participants in this regard.

Communications Alliance's work in reviewing the 2007 Code occurred over an 18 month period, led by a Steering Group comprised of industry representatives, consumer representatives and representatives from the ACMA, the ACCC and the Department of Broadband, Communications and the Digital Economy. The drafting work for what is a considerable document was largely undertaken by six Working Committees comprised of industry and consumer representatives.

Shortly before publication of its draft 2011 Code for public comment, Communications Alliance received a notification from the ACMA under section 125 of the Act indicating the ACMA's view that the 2007 TCP Code was now deficient, with a remedy required by early February 2012. The ACMA's *Reconnecting the Customer* report, discussed in more detail below, presumably indicates the ACMA's views on how the perceived deficiencies ought to be remedied. That said, as the ACMA's public inquiry leading to the *Reconnecting the Customer* report was undertaken at the same time that the Communications Alliance Steering Group and working committees were meeting to devise the 2011 Code, many of the ACMA's concerns regarding advertising practices, product disclosure, performance reporting, expenditure management tools and complaint handling practices had already been included in the 2011 Code.

2011 Code Drafting Overview

Those familiar with the 2007 Code will notice a significant change in the presentation of the 2011 Code. While the same general areas are covered in both versions, the 2011 Code has been substantially rewritten. Indeed it would be true to say that while the 2007 Code had industry participants as its sole audience (for example, customer facing staff within a carrier or carriage service provider), the 2011 Code also addresses the consumer audience.

The drafting style adopted across each of its nine chapters is one of stipulating outcomes, generally commencing with words "a Supplier must ....", followed by considerable detail which establishes the minimum performance requirements and actions of industry participants to achieve these outcomes, including in some cases details of consumer "entitlements".

As noted below, there are a number of areas of the 2011 Code which are either covered for the first time, or to which significant enhancements have been made since the 2007 Code. For instance:

- there is a new compliance framework under the auspices of a new body, Communications Compliance;

- spend management tool obligations on carriage service providers have been significantly extended;
- product disclosure and advertising obligations have been enhanced considerably;
- complaint handling timeframes and obligations have been tightened;
- there are additional obligations regarding vulnerable customers; and
- there is greater emphasis on providing easily accessible consumer information in plain language.

It is important to note that the provisions of the 2011 Code referred to below may change in light of comments made in the public comment period underway at the time of writing.

Consumer Sales Service and Contract

Chapter 4 of the 2011 Code, covering consumer sales, service and contracts, encompasses at least three significant innovations:

Summary of Consumer Offers

A supplier must now provide a summary of each of its then current generally applicable offers to allow consumers to make comparisons. The document is of course different to the summaries required by the Act to be prepared in relation to standard forms of agreement. The contents is prescribed, and will need to include such items as:

- all key pricing information;
- for mobile post paid services, details of the cost of 2 minutes of a standard national mobile call (and an explanation of what constitutes such a call), the cost of a standard national mobile SMS and a similar explanation, and the cost of 1 megabyte of calls, SMS and data usage within Australia;
- details of any inclusions, exclusions, conditions or limitations;
- a "single price", as defined in the CCA;
- explanations of contract expiry or roll over, contract length and exit and termination fees; and
- how to access spend management tools.

It is important to note that for post paid services this document is to be provided prior to sale (with the exception of unsolicited consumer sales), or alternatively consumers can opt out of receiving the document prior to sale (but will still receive it after sale) after having been given a general overview of its contents. The document must also be available online for prepaid offers.

The summary must comprise no more than two A4 pages in plain language, and meet all other requirements under the telecommunications and consumer protection legislative regime. Needless to say, preparing the summary of offers is likely to become an art form in itself as in-house legal advisers and external law firms seek to meet all of the requirements in the space prescribed.

Advertising

Chapter 4 of the 2011 Code also provides some extensive prescriptions for the manner in which telecommunications goods and services may now be advertised. Many of the new requirements substantially reflect an undertaking made by Vodafone, Optus and Telstra to the ACCC in 2009 in relation to advertising. Effectively, that undertaking will now apply to all industry participants.

Importantly, when advertising an "included value" for mobile post paid services in online and print media of certain types and sizes, suppliers must, among other things, disclose the following three standard pricing elements in a prominent position:

- the cost of two minutes of a standard national mobile call;
- the cost of a standard national mobile SMS; and
- the cost of one megabyte of data within Australia.

"Caps"

"Cap" is an expression which has been used for a considerable period of time by the telecommunications industry. During the ACMA's public inquiry and in the research undertaken by the Communication Alliance for the 2011 Code, it became clear that some further clarification was required.

Under the 2011 Code, new products and services which are offered after the date of Code registration must cease to be subject to the expression "cap" unless it is used to describe a "hard cap". A hard cap, for the purposes of the 2011 Code, means a maximum limit applied to a customer's use of telecommunications services where that limit cannot be exceeded. For existing products and services, when advertising caps, suppliers must make it clear that customers may need to pay more that the monthly quoted cap amount.

This arises out of a concern expressed by consumers and regulators alike that "bill-shock" was a significant factor leading to complaints against suppliers by customers

Billing

While a number of the provisions in the billing chapter of the 2011 Code have strong similarities to those found in the 2007 Code, the new provisions apply more extensively to prepaid services. Further, greater historic billing information must be provided to a customer upon request and must be provided in relation to both prepaid and post paid services. It is proposed that billing information must now be provided (if requested) free of charge for 13 months after a charge has been incurred, and then with a fee for another six years.

There is now greater clarity as to what a bill must contain. Bills must include:

- sequential numbers to enable customers to identify chronological order;
- the same customer reference for online payments for each bill if it relates to the same service;
- at least one free bill payment method, with advice provided on charges which will apply to other methods;
- the name of the service to which the bill relates;
- itemisation of charges and identification of charges that exceed spend limits or included allowances and, where exceeded, an explanation of the effect on charging as a consequence;
- an explanation of how to access usage details;
- greater description of charges included in the bill, including total amounts; and
- where the bill relates to a cap plan, the total amount of each of the previous two bills.

Credit and Debt Management

The 2011 Code places a significant emphasis on the provision of spend management tools to consumers. This arises out of a concern expressed by consumers and regulators alike that "bill-shock" was a significant factor leading to complaints against suppliers by customers.

Under the 2011 Code, carriage service providers must provide a comprehensive list of available spend management tools in prominent, easily navigable and searchable positions on their website.

In what will result in a significant investment requirement for carriage service providers, suppliers must now provide mandatory notifications to consumers to enable them to manage their spend on telecommunications services. For residential customers, where the supplier is offering a post paid mobile or internet plan with an included data allowance (and in circumstances where no shaping, throttling or hard caps apply), suppliers must provide customers with a notification once that customer has used:

- 50% of the data allowance included in their plan;
- 80% of that allowance; and
- 100% of that allowance.

In the latter case, the notification must also include information as to whether excess data charges will apply after that time.

These notifications need to be provided no later than 48 hours after the customer has actually reached the relevant usage point. There is provision for opt out and variations with customer express consent. In addition, these reforms do not need to be implemented until, at the latest, 12 months after the 2011 Code is registered.

Another issue which was addressed by the 2007 Code and which has received significant enhancement in the 2011 Code, are the financial hardship obligations which are applicable to suppliers. Suppliers must have a financial hardship policy which is set out in a prominent, easily navigable and searchable position on its website. If a customer wishes to have that policy applied to it, suppliers must assess the eligibility of that customer within seven working days of receiving all the required information from it. Reforms also include providing details of community financial counsellors on the website of a carrier's service provider.

Suppliers must have a financial hardship policy which is set out in a prominent, easily navigable and searchable position on its website

Changing Suppliers

In the preparation of the 2011 Code, a number of participants expressed concern about the amount and timeliness of information provided to consumers when the supplier of services changes.

One issue which was not considered to be adequately addressed in the 2007 Code arises in circumstances where a transfer of a supplier's business has arisen as a result of either a sale or a corporate reorganisation inside the same group of supplier companies. In such circumstances, suppliers now have an obligation to inform customers of any known materially adverse effects, with customers being informed of the ability to terminate their contract with a 30 working day notice period if they wish to do so as a result of the merger or reorganisation.

Complaint Handling

The telecommunications industry has long been served by the Telecommunications Industry Ombudsman (***TIO***) as its key complaint handling body. Indeed, the perceived health or otherwise of the industry is often measured by the rise and fall in the number of complaints made to the TIO.

The obligations on carriers to promote the complaint handling services of the TIO needs, of course, to be balanced with encouraging suppliers to deal with complaints internally before the resources of the TIO are used.

In this regard, the 2011 Code now provides more clarity as to what constitutes a customer complaint (as opposed to a mere inquiry or fault report) and provides some tight timeframes for complaint acknowledgement and resolution by the supplier in the first instance. Examples include:

- the requirement for suppliers to immediately acknowledge a telephone or "in person" complaint, or within two working days for all other complaints;
- these complaint acknowledgements are to include unique reference numbers and identifiers and provide an indicative framework for resolution by the supplier;
- suppliers must finalise complaints within 15 working days from receipt of a complaint, or as soon as practicable in the circumstances; and
- for urgent complaints, suppliers are required to provide written confirmation of the resolution path and set into motion that resolution within two working days.

There are now clear obligations upon the supplier to advise of the complaint outcome and, if requested, to provide a written confirmation of that outcome.

Balancing this increased emphasis on resolution of complaints at the supplier's level, suppliers are also required to explicitly promote the services of the TIO and keep the TIO informed of certain of its complaint handling activities.

Communications Compliance

One of the key innovations of the 2011 Code is a greatly enhanced compliance and monitoring regime. A new independent body, Communications Compliance, has been created to monitor Code compliance by suppliers.

Suppliers will be required to implement and comply with a code compliance framework set out in Chapter 9 of the new Code. In essence, this involves:

- promoting awareness of the Code to its customers;
- preparing an annual statement (a "Customer Information Compliance Statement") which specifies where the supplier's customers may access the supplier's information which is required to be made publicly available under the Code; and
- preparing and maintaining a documented compliance plan which outlines the initiatives of the supplier relating to its compliance with the Code. This plan must be prepared in accordance with the relevant Australian Standard.

In addition, suppliers must provide Communications Compliance with certain prescribed statements, with requirements varying depending on the size of the relevant supplier. In the case of large suppliers (as defined in the Code), these statements require annual attestation of Code compliance, along with a statement from an external qualified assessor that the relevant Australian Standard has been met. Small, medium and new entrant suppliers will also need to provide their compliance attestation to Communications Compliance on an annual basis but these will need to be signed by a chief executive or the board of that supplier.

If the supplier is unable to make the attestations and give the statements referred to above, a new regime will apply pursuant to which that supplier may give "Compliance Achievement Plans" to Communications Compliance detailing how and when actions will be taken to ensure that supplier's compliance.

It is envisaged that Communications Compliance will be governed by a three member board. One board member will be nominated by Communications Alliance and a second will be nominated by consumer representatives, both of whom will then nominate an Executive Director. The day to day affairs of Communications Compliance will again have equal representation from industry and consumers under the direction of that Executive Director.

It is anticipated that Communications Compliance will enter into a Memorandum Of Understanding with each of the TIO, the ACMA and the ACCC to ensure efficient inter-working and to avoid duplication.

Reconnecting The Customer

At around the time the 2011 Code draft was taking its final shape, the ACMA published its *Reconnecting the Customer* final report. With the ACMA having visibility of much of the work of the Communications Alliance Steering Group, it is not surprising that many of the recommendations under the *Reconnecting the Customer* report anticipate and extend upon many of the initiatives in the 2011 Code.

As mentioned above, the ACMA has given clear indication in its section 125 notice that it expects the five key proposals from the Reconnection the Customer report described below to be accommodated in the 2011 Code.

Improved Advertising Practices

The ACMA has focused particularly on the use of the expression "caps". As noted above, this same issue occupied much of the discussion time in the preparation of Chapter 4 of the 2011 Code regarding advertising.

Essentially, for products that are not subject to a hard cap or shaping of data use, the ACMA proposes that suppliers, in text based advertising, clarify minimum monthly spend representations with the inclusion of:

- standardised rates disclosing the cost of making a two minute call in Australia to another mobile (based on the highest rate charged under the plan for making that call, plus flag fall), sending a standard SMS in Australia, and downloading one megabyte of data in Australia; and
- an estimate of the volume of calls included in the plan, based on the standardised rate disclosed and assuming that the value that can be used on either calls or SMS was used on calls only.

Improved Product Disclosure

The ACMA proposes that service providers be required to provide a critical information summary to consumers before a sale that:

- summarises critical information about the product; and
- provides consumers with non product specific information (for example, customer service contact details and how to access spend management tools).

As noted above, this is largely accommodated by the current draft of 2011 Code.

Performance Reporting and Customer Service Charters

The ACMA is seeking industry proposals regarding metrics which can be used to measure customer care performance, including timely complaint resolution, and implementing a metric reporting framework for service providers with more than 30,000 residential or small business customers. It is intended that these metrics will be published.

Chapter 9 of the 2011 Code requires that suppliers provide to Communications Compliance annually, or more frequently if required, a report in a format required by Communications Compliance detailing metrics that relate to that supplier. Those metrics may relate to any of the obligations of the supplier under the Code. The Chapter also requires Communications Compliance to agree to the scope of metrics within six months of Code registration.

Presumably then, this avenue will be used to address this concern of the ACMA. The ACMA has flagged however, that if industry does not implement its own metric reporting framework the ACMA will directly require suppliers to provide it with the required information, including information regarding:

- the total number of contacts made by existing customers;
- the number of repeat contacts made by the same customer within a 45 day period;
- the total number of complaints received by the service provider; and
- the total number of the service provider's residential and small business customers.

Expenditure Management Tools

While the provision of enhanced spend management tools may greatly assist consumers, there is of course a risk that consumers may be inadvertently disadvantaged if such requirements are so burdensome that it effectively forces smaller retailers out of the market (and, as a result, diminishes competition), or if the large costs of implementing these changes is passed on to consumers.

It appears, however, that both Communications Alliance and the ACMA have landed in a similar but not identical position, with the ACMA's proposed expenditure management tools requiring notification via SMS for phone usage, and an email for internet usage that alerts consumers at specific expenditure and usage points (such as 50% or 80%, and at 95%). The alert should also include details about the expenditure or usage point reached and the consequences of any exclusions (such as roaming). The key difference appears to be that the ACMA is seeking notifications in relation to SMS and voice, as well as data (as proposed by the 2011 Code).

Like the 2011 Code, the ACMA's recommendations also require certain historical information to be revealed on bills.

if industry does not implement its own metric reporting framework the ACMA will directly require suppliers to provide it with the required information

External Complaints Handling

Similarly, much of the proposal by the ACMA in relation to internal complaints handling appears to have been addressed by the 2011 Code in Chapter 8.

The ACMA proposes that service providers be required to implement a complaints handling procedure that:

- adopts the definition of a complaint set out in the *Australian Standard for Complaints Handling* (AS ISO 10002-2006). This is expressly achieved by 2011 Code;
- complies with the guiding principles set out in that Australian Standard. This is already addressed by the 2011 Code; and
- establishes minimum benchmarks for ensuring timeliness in dealing with complaints, documenting procedures and collecting, analysing and reporting complaints information.

Changes to the TIO Scheme

Finally, the *Reconnecting the Customer* report recommends some changes to the TIO scheme which are beyond the scope of the 2011 Code. No doubt, however, those proposed changes, if they are implemented, will impact on the proposed Memorandum of Understanding between the new Communications Compliance body and the TIO.

Conclusion

While the gestation period for both the 2011 Code and *Reconnecting the Customer* has been long, the journey to create them has been intertwined and, as a result, the difference between their outcomes is not great.

Whether those differences are, in the view of the ACMA, still sufficient for it to either reject the 2011 Code, excise parts of it and/or implement its own standard is yet to be seen.

Shane Barber is the managing partner of Truman Hoyle Lawyers. Truman Hoyle acts for a number of telecommunications industry participants and was engaged by Communications Alliance to provide drafting services for the 2011 TCP Code.

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 tele-communications 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.

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 editors@camla.org.au or to

Valeska Bloch or Victoria Wark

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

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

Please note the change to CAMLA details:

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

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)

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

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

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

Signature: .....