Communications Law BULLETIN

CAMLA

Communications & Media Law Association Incorporated

Print Post Approved PP: 100001546

The "It's Complicated" Relationship Between Social Media and Australian Copyright Law

Amanda Parks considers copyright laws in the context of social media use and the ALRC's recommended introduction of a flexible fair use exception.

Can the ALRC's fair use exception help?

Following Oxford Dictionaries' decision to crown *selfie* as 'Word of the Year' for 2013, we saw a particularly famous one 'break' Twitter and spark a copyright debate after this year's Oscars awards show (marking quite a change from the ever-so-predictable fashion debate that inevitably follows the event). This year, host Ellen Degeneres shared a star-studded photo that was retweeted over 2 million times in 2 hours, and questions quickly arose as to why the Associated Press sought *her* permission to share it when it was *Bradley Cooper* who pressed the button.

What happens on social media is a hot topic in any discussion about how copyright laws do and should operate in the online world. Only a few months ago, the Australian Law Reform Commission (***ALRC***) concluded its 18-month enquiry entitled *Copyright in the digital economy*, tabling its Final Report in Parliament on 13 February. The ALRC was tasked with considering whether and how the *Copyright Act 1968* (Cth) (***Act***) should be updated to account for developments in the digital space, and it ultimately recommended the introduction of a flexible fair use exception.

While the social media sphere is bursting with benefits for its many users, it can also present a number of challenges for those who are concerned about the potential for their copyright materials to be shared with incredible ease, speed and reach, yet without their consent.

The nature of copyright infringement by the casual social media user

The sharing of content on networks like Facebook and YouTube has spread with great contagion, yet many social media users do not realise that their activities may involve breaches of copyright (however harmless those breaches may seem to some). Copyright concerns can arise when social media users share, as they so often do, content constituting or incorporating all or part of someone else's material. Consider these two recently-observed examples:

Example 1:
Facebook User A posts a status update in the following terms: "*Where do you guys find all of your great cover photos? I often see things that I like when I'm browsing the internet, but I don't want to infringe copyright.*" Facebook User B responds: *"If it's on the internet and it's not watermarked, it's fair game"*. Within a day, User A has thanked User B for the 'advice' and replaced her old photo with an image that has almost certainly been copied from a third party's website.

Example 2:
Another Facebook user celebrates Australia Day by posting an artist's creative image of the Sydney Opera House to her personal page, with the following comment: "*Taking this opportunity to share some love through art. If you like this post, you will receive an artist and will need to*

Volume 33 Nº 2
June 2014

Inside This Issue:

The "It's Complicated" Relationship Between Social Media and Australian Copyright Law

An Overview of Privacy Law in Australia: Part 2

Exercising Jurisdiction Over Foreign Corporations: The USA PATRIOT Act and the Extent to Which US Government Law Enforcement Agencies can Obtain Information from Abroad

Profile: Fiona Lang COO of BBC Worldwide Australia

The Deregulation Agenda for Australian Media Ownership: Can Competition do the Heavy Lifting?

Contents

The "It's Complicated" Relationship Between Social Media and Australian Copyright Law
Amanda Parks considers copyright laws in the context of social media use and the ALRC's recommended introduction of a flexible fair use exception.

An Overview of Privacy Law in Australia: Part 2
In the second of a two part special, Peter Leonard provides a thoughtful commentary on privacy reforms. In Part 1 published in the previous edition, he provided a high level overview of the amendments to the Privacy Act 1988 and the new Australian Privacy Principles. In this Part 2, he provides an in depth analysis of Australia's privacy regime, focusing on the APPs, the regulation of privacy beyond the Privacy Act 1988, issues of extraterritoriality and emerging trends and issues.

Exercising Jurisdiction Over Foreign Corporations: The USA PATRIOT Act and the Extent to Which US Government Law Enforcement Agencies can Obtain Information from Abroad
Ken Wong considers the implications of the PATRIOT Act on the ability of US Government law enforcement agencies to obtain information from abroad.

Profile: Fiona Lang - COO of BBC Worldwide Australia
In a new feature for the Communications Law Bulletin, Daniel Doctor, a member of CAMLA's young lawyers committee, chats to Fiona Lang, the new COO of BBC Worldwide Australia and New Zealand, about her new role and what she sees as the key challenges and trends in the Australian media industry.

The Deregulation Agenda for Australian Media Ownership: Can Competition do the Heavy Lifting?
In light of recent comments from the Communications Minister, Barry Dean, Jennifer Dean and Shyla Sharma consider the potential impact of reform of Australian media ownership regulation.

post an image of his/her art. Let's share some art love." Predictably, this receives several 'likes' from other users who continue to post the works of their allocated artists, and so the snowball rolls on…

there is often a disconnect between what the law actually allows and what the average person thinks or assumes is allowed

Most likely, these Facebook users would be found to have infringed copyright in the works they shared because their conduct does not fit within an existing fair dealing exception in the Act, such as use for the purpose of criticism or review (sections 41 and 103A) or parody or satire (sections 41A and 103AA). Equally likely is the probability that these participants are completely unaware that their conduct amounts to an infringement of someone else's rights; these examples illustrate the point made by many who support the introduction of a flexible fair use exception, which is that there is often a disconnect between what the law actually allows and what the average person thinks or assumes is allowed.

One of the questions that have been so hotly debated in recent months is this: should these types of content-sharing activities constitute copyright infringement? Many have argued not, insisting that Australian copyright laws should be updated to better reflect the reasonable expectations of the public, as well as the realities of participation in the online world. This begs the next question: would these types of content-sharing activities constitute infringement under the ALRC's proposed fair use exception?

The proposed exception

In its Final Report, the ALRC recommended the introduction of a flexible fair use exception that should include:

1 an express statement that a fair use of copyright material does not infringe copyright.

2 a non-exhaustive list of 'fairness factors' to be considered in determining whether a use is fair, being the:

   (a) purpose and character of the use;

   (b) nature of the copyright material;

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

   (d) effect of the use upon the potential market for, or value of, the copyright material; and

3 a non-exhaustive list of illustrative uses or purposes that may qualify as fair use, including research or study; criticism or review; parody or satire; reporting news; professional advice; quotation; non-commercial private use; incidental or technical use; library or archive use; education; and access for people with disability.

The proposed fair use exception expands the permissible uses of copyright material beyond those that are currently provided for in the Act's fair dealing provisions. Those provisions provide exceptions for the purposes of research or study, criticism or review, parody or satire, reporting news and professional advice, but they are closed-ended, prescriptive exceptions that require a use of copyright material to be for one of these specific purposes. In contrast, the proposed fair use exception involves an open-ended, principles-based approach to assessing whether a use of copyright material is fair, having regard to the 'fairness factors' and with reference to the 'illustrative purposes' for which a particular use is more likely to be considered fair.

Interestingly, 'social use' was deliberately excluded from the 'illustrative purposes' list; the ALRC considered that social use will often not be fair, particularly where it harms rights holders' markets and is not 'transformative' (meaning use for a different purpose than that for which the material was created). The ALRC also clarified that social use should not be interpreted as falling within the category of 'non-

The proposed fair use exception expands the permissible uses of copyright material beyond those that are currently provided for in the Act's fair dealing provisions

commercial private use' because many social uses will not in fact be private (citing as examples the acts of sharing copyrighted songs or videos on YouTube or Facebook).

Nevertheless, the ALRC indicated that certain social uses of copyright material (particularly transformative uses) may be fair, such as use for the purpose of creating and sharing user-generated content. A particularly popular type of user-generated content is the meme, a classic example of which is 'Grumpy Cat.' For those who have managed to miss this, it involves a photo of a cat overlaid with varying comedic captions playing on the cat's less-than-impressed facial expression. Currently, the act of sharing 'Grumpy Cat' with 800 Facebook friends might be an exception to infringement if it can be viewed as a parody or satire, but not all memes can be so classified. Under the proposed fair use exception, there would be more scope for this to be considered an exception, as the primary question would not be whether the meme is a parody or satire, but rather, whether the use of the relevant copyright work is fair.

Ultimately, the ALRC concluded that social use must be considered on a case-by-case basis by reference to the fairness factors.

What next

It is unclear when the government will formally respond to the ALRC's Final Report, but Attorney General George Brandis delivered a speech to the Australian Digital Alliance on 14 February in which he said he remains unpersuaded that a fair use exception is the best direction for Australian law (though he maintained that he will "bring an open and inquiring mind to the debate").

Given that the posting and sharing of copyright materials via social media is unlikely to abate, copyright owners should evaluate how, or even whether, they should take action. Some might consider taking proactive steps to prevent their content from being shared, such as displaying copyright notices on websites or applying watermarks to images. Others may actually benefit from having their work shared by and between hundreds or thousands (or even millions) of users on social networks; there is arguably no better advertising and no faster way to be 'discovered.' Those eager to share their work may want to consider making it available via Creative Commons; there are several standard licences which allow artists to select the terms upon which they are content for their works to be shared, and help to ensure that those who make their works available are appropriately credited.

While we wait to see whether the proposed fair use exception will become law, it is worth evaluating whether something can be gained by swimming *with*, not *against*, the social media current.

Amanda Parks is an Associate at Norton Rose Fulbright.

CAMLA's Annual Trivia Night is on the approach!

Start hitting the books and NW Magazine now!

Thursday 14th August
6:00pm for 6:30pm start

NSW Leagues' Club
Level 2, 165 Phillip St
SYDNEY

CAMLA members to receive further information shortly but please register your early interest by emailing camla@tpg.com.au

An Overview of Privacy Law in Australia: Part 2

In the second of a two part special, Peter Leonard provides a thoughtful commentary on privacy reforms. In Part 1 published in the previous edition, he provided a high level overview of the amendments to the Privacy Act 1988 and the new Australian Privacy Principles. In this Part 2, he provides an in depth analysis of Australia's privacy regime, focusing on the APPs, the regulation of privacy beyond the Privacy Act 1988, issues of extraterritoriality and emerging trends and issues.

Communications, Surveillance, Marketing and Other Laws

It is important to note the limited coverage of Australian Federal privacy law. There is at present no common law right of action in Australia for intrusion upon an individual's seclusion or private affairs or for misuse or disclosure of private information. The Federal Privacy Act 1988 (the ***Privacy Act***) and some State and Territory Acts regulate the use by government agencies and many businesses of personal information as embodied in particular records. This is really a sub-category of private information that is personally information collected into a material form, such as a record, for use by regulated businesses and government. Some modes of invasion upon personal seclusion or private affairs are specifically regulated. There are a number of subject matter specific federal and state laws governing telecommunications interception (including access to stored communications such as emails), employee, optical (including video) surveillance, workplace surveillance and the use of recording devices, listening devices and tracking devices.

State and territory statutes dealing with interception, monitoring and surveillance laws vary substantially, both in scope of coverage and drafting

Certain forms of unsolicited marketing are also specifically regulated. New APP 7 regulates use or disclosure of personal information for the purpose of direct marketing activities. Direct marketing involves the use or disclosure of personal information to communicate directly with an individual to promote goods and services. A direct marketer may communicate with an individual through a variety of channels, including telephone, SMS, mail, email, online advertising and social media. Key factors in applying APP 7 are:

- ensuring that sensitive information is not used (unless there is express opt-in consent) for direct marketing;
- determining whether a particular marketing activity is 'direct marketing' that is regulated by APP 7;
- determining whether the *Spam Act 2003* (Cth) (***Spam Act***) or the *Do Not Call Register Act 2006* (Cth) (***DNCR Act***) apply to regulate the particular activity, such that APP 7 does not apply (because an exception in APP 7.8 operates); and

determining whether the organisation collected the personal information from the individual in circumstances where the individual would reasonably expect the organisation to use or disclose the personal information for the purpose of direct marketing; or whether the individual would not reasonably expect their information to be used or disclosed for that purpose or the information was collected from a third party.

APP 7 requires the direct marking organisation to provide a simple way for the individual to request not to receive direct marketing communications from the organisation. There must be a visible, clear and easily understood explanation of how to opt out and a process for opting out which requires minimal time and effort that uses a straightforward communication channel accessible at no more than nominal cost. In addition, in any circumstance where the individual would not reasonably expect their information to be used or disclosed for the purpose of direct marketing or personal information about them was collected from a third party, in each direct marketing communication with the individual the organisation must include a prominent statement ('opt out statement'), or otherwise draw the individual's attention to the fact, that the individual may request an opt-out.

Other instruments dealing with electronic marketing, interception, monitoring and surveillance, include the following:

- *the Spam Act 2003* (Cth) (***Spam Act***), which deals with the sending of unsolicited commercial electronic messages, including emails and SMS;
- *the Do Not Call Register Act 2006* (Cth) (***DNCR Act***), which regulates unsolicited commercial calling to telephone numbers listed on the national Do Not Call Register and imposes certain conditions as to telemarketing generally (including as to time of day of calling);
- eMarketing Code of Practice, which contains rules and guidelines for the sending of commercial electronic messages. The Code is given legal effect by registration of that Code with the Australian Communications and Media Authority (***ACMA***);
- *Telecommunications (Interception and Access) Act 1979* (Cth), which among other things, regulates the interception of, and access to, stored communications by law enforcement agencies;
- a range of federal and state and territory statutes governing the use of listening devices and workplace surveillance;
- a more limited range of federal and state and territory statutes governing the use of unauthorised optical surveillance and tracking devices;
- state and federal criminal law provisions dealing with unauthorised access to computer systems; and
- the Australian Guideline for Third Party Online Behavioural Advertising.

The Spam Act prohibits 'unsolicited commercial electronic messages' with an 'Australian link' from being sent or caused to be sent. Com-

mercial electronic messages may only be sent with an individual's consent (express or implied in certain circumstances) and where the message contains accurate sender identification and a functional unsubscribe facility.

The Spam Act defines a 'commercial electronic message' as any electronic message (including e-mail, SMS, multimedia messages, instant messages or any other direct electronic messaging) where having regard to:

- the content of the message;
- the way in which the message is presented; and
- content that can be accessed by following any links, phone numbers or contact information in the message,

it could be considered that a purpose, or one of the purposes, of the message is to:

- offer, advertise or promote the supply of goods, services, land or business or investment opportunities;
- advertise or promote a supplier of goods, services, land or a provider of business or investment opportunities; or
- assist or enable a person to dishonestly obtain property, commercial advantage or other gain from another person.

Any electronic message that passes this test of commerciality is caught by the Spam Act (subject to certain exceptions). Commerciality may be a secondary purpose: for example, if a message is mainly factual or useful information, but has some marketing or promotional content, it is a commercial electronic message.

A message has an 'Australian link' if it originates or was commissioned in Australia, or originates overseas but was sent to an address accessed in Australia. The Spam Act expressly includes e-mails, SMS, instant messages and MMS. Whether the Spam Act can be applied to social media postings is less clear: although these may not be 'electronic messages' within the meaning of the Act, this position has not been tested.

Voice calls, including synthetic or recorded calls (such as robocalls), are separately regulated under a 'do not call' regulatory framework established under the DNCR Act and associated legislation and instruments, including the important *Telecommunications (Do Not Call Register) (Telemarketing and Research Calls) Industry Standard* 2007.

Marketing faxes are regulated under the DNCR Act. This Act provides an 'opt-out' framework for these forms of marketing. Unsolicited telemarketing calls or faxes must not be made to an Australian number registered on the Do Not Call -Register.

The Spam Act and the DNCR Act are administered by the ACMA. Extensive material as to the operation of these statutes and enforcement activity by the ACMA is available at www.acma.gov.au.

State and territory statutes dealing with interception, monitoring and surveillance laws vary substantially, both in scope of coverage and drafting. There are important inconsistencies both in scope of coverage and treatment of technologies that are covered. Tracking device law makes it an offence in some states to track movement of devices even where there is no identification of the owner of those devices or their communications activities: this appears a simple overreach of regulation that potentially obstructs many benign new users of tracking for logistics, store traffic analysis and transport planning. In any event, surveillance laws do not provide nationally coherent coverage or comprehensive rights of seclusion for individuals. In addition, , many computer crime, unauthorised computer access, tracking devices and surveillance provisions were not drafted with regard to current applications of the internet and mobile devices and are therefore difficult to interpret and apply.

Other specific data protection rules in areas related to privacy include:

- Part 13 of the *Telecommunications Act 1997* (Cth), which imposes restrictions on the use and disclosure of telecommunications and communications-related data;
- state and territory privacy legislation, applying to personal information held by government agencies and, in some cases, health information and records (for example, the *Privacy and Personal Information Protection Act 1988* (NSW));
- the *Healthcare Identifiers Act 2010* (Cth), regulating (among other things) the use and disclosure of healthcare identifiers;
- the *Data-matching Program (Assistance and Tax) Act 1990* (Cth), which regulates federal government data-matching using tax file numbers;
- the *Personally Controlled Electronic Health Records Act 2012* (Cth), which provides strict controls on the collection, use and disclosure of health information included in an individual's eHealth record; and
- federal and state/territory freedom of information legislation applying to information held by government agencies.

There is no legislation in Australia similar to the US Federal *Children's Online Privacy Protection Act of 1998* (***COPPA***), although COPPA principles are commonly applied in Australia as a matter of good corporate practice.

Privacy regulation operates up to the point at which personal information is transformed such that any risk that the information might either of itself, or in combination with other information, enable an individual to be identifiable becomes effectively impracticable

One of the few areas of clear and nationally consistent industry sector specific regulation is as to media reporting: there is a general carve out in the (Federal) Privacy Act for journalism by media organisations that self-regulate privacy compliance in their reporting, such as through the Statement of Privacy Principles administered by the Australian Press Council and the electronic broadcasting codes of practice overseen by the Australian Communications and Media Authority. However, the extent of that exception has itself been controversial: hence the continuing demands of privacy advocates for a broader right of seclusion and the countervailing media concerns as to freedom of reporting.

Personal Information

Generally, the (Federal) Privacy Act covers all processing (in Australian terms, itself a 'use') or use of 'personal information'.

The Act makes no express distinction between entities that control or own personal information, and those that provide services to owners (except in the case of contracted service providers to public-sector agencies). All such entities are regulated as APP entities in respect of their handling of personal information.

The definition of 'personal information' from March 2014 extends to information or an opinion about an individual who is reasonably identifiable, whether or not the information or opinion is recorded in a material form (this includes information communicated verbally) and regardless of whether that identification or re-identification is practicable from the information itself or in combination with or reference to other information.

Personal information will therefore include information about an individual whether collected or made available in a personal or business context and regardless of whether that information is in the public domain and the subject individual is specifically identified or consented for that information to enter the public domain.

Personal information remains such while identification or re-identification of an individual is 'practicable' either from the information itself or by reference to that information in combination with or by reference to other information. Privacy regulation operates up to the point at which personal information is transformed such that any risk that the information might either of itself, or in combination with other information, enable an individual to be identifiable becomes effectively impracticable. That transformation might be through aggregation or anonymisation of the personal information. Many organisations maintain multiple transaction databases, some of which may include personal information and some of which may include transaction data that does not identify a particular individual undertaking a transaction. These databases may be partitioned so that the non-identifying transactional database is not matched against the databases containing personal information. Partitioning of databases within organisations will be ineffective to allow non-identifying transactional data to be used without complying with the rules that relate to use of personal information, wherever there is any way in which an individual could be matched and tied to non-identifying transaction data, because the individual remains 'reasonably identifiable'. The Privacy Commissioner's February 2014 Guidelines put it this way:

APP 8, which deals with the cross-border disclosure of personal information from Australia to outside Australia, is not limited in its application by the nationality of the individual whose personal information is the subject of the transfer

> B.87 Whether a person is 'reasonably identifiable' is an objective test that has practical regard to the context in which the issue arises. Even though it may be technically possible to identify an individual from information, if doing so is so impractical that there is almost no likelihood of it occurring, the information would not generally be regarded as 'personal information'. An individual may not be reasonably identifiable if the steps required to do so are excessively time-consuming or costly in all the circumstances.
>
> B.88 Where it is unclear whether an individual is 'reasonably identifiable', an APP entity should err on the side of caution and treat the information as personal information.

This view reflects regulatory guidance in some jurisdictions to the effect that determination as to whether information is 'personal information' is to be made having regard to all relevant circumstances as to possible re-identification by any reasonably contemplated recipient, or as it is sometimes put, to be made 'in the round', rather than having regard to whether the information was passed to the first recipient in apparently de-identified form. In assessing the risk of re-identification, regulatory guidance in some jurisdictions suggests that risk management strategies – or as it is sometimes put, technical, operational and contractual safeguards – are to be taken into account. The United Kingdom regulator suggests a 'motivated intruder' test: this test considers whether a reasonably competent motivated person with no specialist skills would be able to identify the data or information, having access to resources such as the internet and all public documents and making reasonable enquiries to gain more information.

Extraterritoriality

The Privacy Act applies to all acts or practices within Australia in respect of personal information about individuals wherever those individuals may reside. Accordingly, personal information of persons outside Australia that is held on servers located within Australia is regulated by the Act.

The Privacy Act extends to any use outside Australia or disclosure from Australia of personal information that has been collected within Australia, although the extraterritorial application of the Act in this area is subject to some uncertainty.

The Privacy Act has express extraterritoriality provisions, based upon a nexus of 'Australian link'. In general, corporations incorporated in Australia and Australian incorporated or constituted bodies are deemed to have an Australian link. The Act applies to an act or practice wherever done outside Australia by an agency (broadly, an Australian federal government entity). The Act also applies in relation to an act or practice outside Australia of an organisation or small business operator wherever that organisation or small business operator has a relevant 'Australian link'. However, a small business operator is regulated in relation to an act or practice outside Australia only to the extent similarly regulated in Australia.

Corporations and other bodies and agencies that do not fall into the above categories - broadly, any foreign corporation or body - will be regulated where: (1) the organisation carries on business in Australia; and (2) the personal information was collected or held by the organisation in Australia, either before or at the time of the act or practice.

The collection of personal information 'in Australia' includes the collection of personal information from an individual who is physically within the borders of Australia, or an external territory, by an overseas entity. The Explanatory Memorandum to the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* states that a collection is taken to have occurred 'in Australia' where an individual is physically located in Australia or an external Territory and personal information is collected from that individual via a website and the website is hosted outside of Australia and owned by a foreign company that is based outside of Australia and that is not incorporated in Australia. The Explanatory Memorandum goes on to state that for the operation of the Act, entities such as those described in the last sentence who have an online presence (but no physical presence in Australia) and collect personal information from people who are physically in Australia, carry on a 'business in Australia or an external Territory'. However, this interpretation is not supported by a plain reading of the Act and prior Australian jurisprudence (as to other statutory provisions) concerning 'carrying on business in Australia'. Accordingly, the operation of the Privacy Act in this scenario (without other factors indicating business presence in Australia) should be considered currently uncertain and potentially contentious.

An overseas act or practice (that takes place outside Australia and its external Territories) will not breach the APPs, an approved APP Code, or interfere with an individual's privacy, if the act or practice is required by an applicable foreign law. However, a similar act or practice within Australia pursuant to compulsion of an applicable foreign law is not excused from breach of the APPs or an approved APP Code, or from being an interference with an individual's privacy.

It is also important to note that APP 8, which deals with the cross-border disclosure of personal information from Australia to outside Australia, is not limited in its application by the nationality of the individual whose personal information is the subject of the transfer. In other words, APP 8 will apply to a cross-border disclosure of personal information collected in Australia, irrespective of whether the information relates to an Australian citizen or Australian resident or not.

Regulation of Collection, Use and Disclosure of Personal Information

The Privacy Act requires that the collection, use and disclosure of personal information must be justified on specific grounds.

An organisation must have an APP-compliant privacy policy that contains specified information, including the kinds of personal information it collects, how an individual may complain about a breach of the APPs, and whether the organisation is likely to disclose information to overseas recipients.

An organisation also needs to take reasonable steps to make its APP privacy policy available free of charge and in an appropriate form.

APP 1 also introduces a positive obligation for organisations to implement practices, procedures and systems that will ensure compliance with the APPs and any registered APP codes. APP 1 requires organisations to have ongoing practices and policies in place to ensure that they manage personal information in an open and transparent way. 'Transparent' is not defined, but as used in the Australian Consumer Law, a contractual term is 'transparent' if it is expressed in reasonably plain language, legible, presented clearly and readily available to the person affected by the term. The positive obligation for organisations to implement practices, procedures and systems has been suggested to require implementation of privacy assurance practices and procedures – so-called 'Privacy by Design' principles - into business processes and products.

APP 3 outlines when and how an organisation may collect personal and sensitive information that it solicits from an individual or another entity. An organisation must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the organisation's functions or activities.

APP 3 clarifies that, unless an exception applies, sensitive information must only be collected with an individual's consent if the collection is also reasonably necessary for one or more of the organisation's functions or activities.

An organisation must only collect personal information from the individual, unless it is unreasonable or impracticable to do so.

APP 4 creates obligations in relation to the receipt of personal information which is not solicited. Where an organisation receives unsolicited personal information, it must determine whether it would have been permitted to collect the information under APP 3. If so, APPs 5 to 13 will apply to that information. If the information could not have been collected under APP 3, the organisation must destroy or de-identify that information as soon as practicable, but only if it is lawful and reasonable to do so.

APP 5 specifies certain matters about which an organisation must generally make an individual aware, at the time, or as soon as practicable after, the organisation collects their personal information.

In addition to other matters listed in APPs 1.4 and 5.2, APP 5 requires organisations to notify individuals about the access, correction and complaints processes in their APP privacy policies, and also the location of any likely overseas recipients of individuals' information.

APP 6 outlines the circumstances in which an organisation may use or disclose the personal information that it holds about an individual. If an organisation collects personal information about an individual for a particular purpose (the primary purpose), it must not use or disclose the information for another purpose (the secondary purpose) unless the individual consents to the use or disclosure, or another exception applies.

Additional protections apply to the collection, use and disclosure of a subcategory of personal information called 'sensitive information', which the Privacy Act defines as information or an opinion about an individual's:

- racial or ethnic origin;
- political opinions;
- membership of a political association;
- religious beliefs or affiliations;
- philosophical beliefs;
- membership of a professional or trade association;
- membership of a trade union;
- sexual orientation or practices; or
- criminal record,

which is also personal information; and

- health information about an individual;
- genetic information about an individual that is not otherwise health information;
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- biometric templates.

An organisation must not collect an individual's sensitive information unless an exception applies. Sensitive information may be collected about an individual with consent and if the information is reasonably necessary for one or more of the organisations activities or functions. Further, an organisation may collect sensitive information if required or authorised by or under an Australian law or a court/tribunal order or in certain permitted health situations, such as where the entity reasonably believes that the collection is necessary to lessen or prevent a serious threat to the life, health or safety of any individual or to public health or safety.

The positive obligation for organisations to implement practices, procedures and systems has been suggested to require implementation of privacy assurance practices and procedures – so-called 'Privacy by Design' principles - into business processes and products

The Privacy Act also contains special provisions that apply to personal information included in individuals' credit information files or in credit reports, including information about an individual's repayment history. These provisions also provide for consumer protection in relation to processes dealing with notification, data quality, access and correction and complaints.

The Privacy Act also provides for the making of guidelines by the Commissioner concerning the collection, storage, use and security of tax file number information. Compliance with the Tax File Number Guidelines is mandatory for all tax file number recipients.

APP 6 (Use and disclosure) generally restricts the use and disclosure of personal information to the primary purpose for its collection or related secondary purposes within the exceptions discussed above. A user may consent to other uses or disclosures.

Further restrictions on the disclosure of credit-related personal information are set out in the credit reporting provisions of the Privacy Act. Such disclosure restrictions include the following:

- a credit reporting body must not disclose personal information contained in an individual's credit information file to a third party unless one of the specified exceptions applies (such as where the information is contained in a credit report given to a credit provider for the purpose of assessing an application for credit by the individual); and
- a credit provider must not disclose any personal information in a credit report to a third party for any purpose (subject again to specified exceptions).

The Act also imposes specific restrictions on the disclosure of personal information from within Australia to outside Australia, as discussed below in the section on cross-border disclosure.

'Openness' and Notification

APPs 1 and 5 impose 'openness' requirements in relation to collection of personal information.

An APP entity must take reasonable steps to notify an individual, or otherwise ensure that the individual is aware, that its APP-compliant privacy policy contains information about how to access and seek correction of personal information, and information about the organisation's complaints process; and whether it is likely to disclose an individual's personal information to overseas recipients and, if it is practicable, to specify the countries in which those recipients are likely to be located. If it is not practicable to specify the countries in the notification, the organisation may make the individual aware of them in another way.

Notification obligations arise under the Privacy Act at the point of collection of personal information by an organisation, whether collected directly from the individual or obtained from a third party. If the organisation collects the personal information from someone other than the individual, or the individual may not be aware that the organisation has collected the personal information, it must also take reasonable steps to notify an individual, or otherwise ensure that the individual is aware:

- that the organisation collects or has collected the information, and
- of the circumstances of that collection (APP 5.2(b)).

Notification obligations arise under the Privacy Act at the point of collection of personal information by an organisation, whether collected directly from the individual or obtained from a third party

Some notification requirements may be addressed through the publication of a privacy policy. Specifically, APP 1.4 requires APP entities collecting personal information to specify the following matters in their privacy policy:

- the kinds of personal information that the entity collects and holds;
- how the entity collects and holds personal information;
- the purposes for which the entity collects, holds, uses and discloses personal information;
- how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;
- how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;
- whether the entity is likely to disclose personal information to overseas recipients;
- if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

More specific notification requirements are stated in APP 5. At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps as are reasonable in the circumstances to notify the individual of such matters referred to in subclause 5.2; or to otherwise ensure that the individual is aware of any such matters. The matters referred to in subclause 5.2 are:

- the identity and contact details of the APP entity;
- if the APP entity collects the personal information from someone other than the individual; or the individual may not be aware that the APP entity has collected the personal information, the fact that the entity collects or has collected the information and the circumstances of that collection;
- if the collection of the personal information is required or specifically authorised by Australian law or court order, details about that;
- the purposes for which the APP entity collects the personal information;
- the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;
- any other person, or the types of persons, to which the APP entity usually discloses personal information of the kind collected by the entity;
- that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information;
- that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the APPs, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;
- whether the APP entity is likely to disclose the personal information to overseas recipients;
- if the APP entity is likely to disclose the personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

Use or disclosure of personal information for a purpose other than the primary purpose of collection (being a 'secondary purpose') is permitted under specific exceptions where that secondary use or disclosure is:

- required or authorised by or under an Australian law or a court order;
- necessary to lessen or prevent a serious threat to any individual's life, health or safety, or to public health or safety, and it is unreasonable or impracticable to obtain the consent of the individual;
- necessary in order for an organisation to take appropriate action in relation to a reasonable suspicion of unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities. APP 6.2(e) also permits the use or disclosure of personal information for a secondary purpose to an enforcement body for one or more enforcement related activities;
- in the conduct of surveillance activities, intelligence gathering activities or monitoring activities, by a law enforcement agency;
- the conduct of protective (for example, in relation to children) or custodial activities;
- to assist any APP entity, body or person to locate a person who has been reported as missing (where the entity reasonably believes that this use or disclosure is reasonably necessary, and where that use or disclosure complies with rules made by the Commissioner);
- for the establishment, exercise or defence of a legal or equitable claim; and
- for the purposes of a confidential alternative dispute resolution process.

Generally notification is required wherever a use or disclosure of personal information is made, unless a specific exception applies.

Control of Use

There are a number of provisions in the Privacy Act which directly, or indirectly, enable individuals to exercise a degree of choice or control over use of their personal information by organisations.

For example:

- APP 1 (Openness and transparency), which requires organisations to have ongoing practices and policies in place to ensure that they manage personal information in an open and transparent way;
- APP 2 (Anonymity and pseudonymity), which requires that an organisation provide individuals with the option of dealing with it using a pseudonym or anonymously. Both requirements are subject to certain limited exceptions, including where it is impracticable for the organisation to deal with an individual who has not identified themselves, or where the law or a court/tribunal order requires or authorises the organisation to deal with individuals who have identified themselves;
- APP 3 (Collection of solicited personal information), which clarifies that, unless an exception applies, sensitive information must only be collected with an individual's consent and if the collection is also reasonably necessary for one or more of the organisation's functions or activities;
- APP 5 (Notification), which requires organisations to notify individuals about the access, correction and complaints processes in their APP privacy policies, and also the location of any likely overseas recipients of individuals' information;
- APP 7 (Direct marketing), which requires the availability of opt-out mechanisms in relation to direct marketing;
- APP 12 (Access), which requires an organisation to give an individual access to the personal information that it holds about that individual, unless an exception applies. There is a new express requirement for organisations to respond to requests for access within a reasonable period. In addition, organisations must give access in the manner requested by the individual if it is reasonable to do so. If an organisation decides not to give an individual access, it must generally provide written reasons for the refusal and information about the mechanisms available to complain about the refusal; and
- APP 13 (Correction), which requires an organisation to take reasonable steps to correct personal information to ensure that, having regard to a purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading, if either the organisation is satisfied that it needs to be corrected, or an individual requests that their personal information be corrected. Organisations generally need to notify other APP entities that have been provided with the personal information of any correction, if that notification is requested by the individual.

Data accuracy

APP 10 (Integrity) requires an organisation to take reasonable steps to ensure that the personal information that it collects is accurate, up-to-date and complete.

In relation to use and disclosure, the APP 10 requirement is that an organisation will need to take reasonable steps to ensure that the personal information is relevant (in addition to being accurate, up-to-date, and complete), having regard to the purpose of that use or disclosure.

APP 13 (Correction) requires an organisation to take reasonable steps to correct personal information to ensure that, having regard to a purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading, if either the organisation is satisfied that it needs to be corrected, or an individual requests that their personal information be corrected. Organisations generally need to notify other APP entities that have been provided with the personal information of any correction, if that notification is requested by the individual.

Amount and Duration of Data Holding

There are no express restrictions as to the quantity of personal information an organisation may collect or hold, but organisations are prohibited from collecting and holding personal information unless the information is reasonably necessary for one or more of the organisation's functions or activities.

In addition, where the personal information is sensitive information, organisations are prohibited from collecting and holding that sensitive information unless the individual consents and the information is reasonably necessary for one or more of the organisation's functions or activities or if an exception applies.

APP 11.2 requires an APP entity to take reasonable steps to destroy or de-identify personal information if the organisation no longer needs it for any for which it may be used or disclosed in accordance with the APPs. There are two exceptions to this requirement: if the personal information is contained in a Commonwealth record, or if the organisation is required by or under an Australian law or a court order to retain the information.

Finality Principle

European privacy lawyers sometimes refer to a 'finality principle', to the effect that use and disclosure of personal information is limited by the purposes for which it was originally collected (subject to various exceptions). The concept is that organisations cannot change their minds about the uses they (or others) wish to make of personal information, after the event of collection.

The Australian Law Reform Commission (ALRC) recommended the introduction of a mandatory data breach notification scheme in its 2008 report

The 'finality principle' is partially reflected in APP 6 (Use or disclosure). If an APP entity holds personal information about an individual that was collected for a particular purpose (the ***primary purpose***), the entity must not use or disclose the information for another purpose (the ***secondary purpose***) unless the individual has consented to the use or disclosure of the information; or an exception in subclause 6.2 or 6.3 applies.

Exceptions include:

- the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is, if the information is sensitive information, directly related to the primary purpose; or if the information is not sensitive information, related to the primary purpose;
- the use or disclosure of the information is required or authorised by or under an Australian law or a court order;
- the use or disclosure of the information is necessary to lessen or prevent a serious threat to any individual's life, health or safety, or to public health or safety, and it is unreasonable or impracticable to obtain the consent of the individual;
- the use or disclosure of the information is necessary in order for an organisation to take appropriate action in relation to a reasonable suspicion of unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities; or
- the individual has consented to the use or disclosure.

An APP entity may also use or disclose personal information for the secondary purpose of direct marketing subject to the prescriptive requirements of APP 7.

Data Security and Notification of Data Breaches

APP 11 (Security) requires organisations to take reasonable steps to protect personal information from misuse, interference and loss and unauthorised access, modification or disclosure. When personal information is no longer needed for an authorised purpose by an organisation, it must take reasonable steps to destroy or permanently de-identify it.

Reasonable steps in relation to protection of personal information will vary with the circumstances. Relevant circumstances include (by way of non-exhaustive examples) how sensitive the personal information is, how it is stored (e.g. paper or electronically), the likely harm to the data subject if a breach occurred and the size of the organisation. Similarly, destruction or de-identification processes will vary. In any event, personal information should be destroyed securely and de-identified such that the data subject's identity is no longer reasonably ascertainable from the personal information.

In April 2013, the Office of the Australian Information Commissioner (***OAIC***) published a guide to information security which discusses some of the circumstances that the OAIC takes into account when assessing the reasonableness of the steps taken by entities to ensure information is kept secure. This guide presents a set of non-exhaustive steps and strategies that may be reasonable for an entity to take in order to secure personal information. The OAIC has stated that the Commissioner will refer to this guide when assessing an entity's compliance with security obligations in the Privacy Act.

The transfer of personal information to entities providing outsourced processing services in Australia, therefore, constitutes a disclosure of personal information for the purposes of the Privacy Act

The Privacy Act does not presently impose obligations on agencies or organisations to notify either the OAIC, or the individual concerned, of security breaches involving personal information.

However, the OAIC recommends notification in its guidelines on this area 'Data Breach Notification: A guide to handling personal information security breaches, April 2012'. These guidelines are generally followed by corporations in Australia.

The Australian Law Reform Commission (ALRC) recommended the introduction of a mandatory data breach notification scheme in its 2008 report, 'For Your Information: Australian Privacy Law and Practice'. In 2013, the then federal government introduced the Privacy Amendment (Privacy Alerts) Bill 2013. This Bill had not been passed by both Houses of the Federal Parliament when the Parliament was prorogued and accordingly lapsed. If enacted, this Bill would have built upon the OAIC's scheme of voluntary notification of serious data breaches by entities, as set out in the OAIC's guidelines. The Bill proposed a high threshold based on a reasonable belief by the entity concerned that the data breach is sufficiently serious to pose a real risk of serious harm to affected individuals. In the event of such a breach, the provisions of the Bill, if enacted, would have required the entity to notify affected individuals and the Information Commissioner as soon as practicable. The provisions of the Bill would require that the data breach notice include:

- the identity and contact details of the entity;
- a description of the breach;
- the kinds of personal information concerned;
- recommendations about the steps that individuals should take in response to the breach; and
- any other information specified in any made regulations under the Bill (if enacted).

As at May 2014, it was not clear whether the Coalition Government would re-introduce data breach notification legislation.

Data Protection Officer

Australia has no mandatory requirement to appoint a data protection officer.

It is becoming more common for major corporations to appoint a privacy professional, generally working within a legal or regulatory compliance team. However, there is no legal obligation to do so.

Record Keeping

There is no general requirement as to record keeping. However, the Privacy Act does require an organisation to keep a written note of any use or disclosure of personal information where the organisation reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Written notes must also be made in relation to certain uses or disclosures of credit related personal information, including the use and disclosure of such information for direct marketing pre-screening assessments.

Further, reasonable steps under APP 11 (Security) may require certain processes to be established, depending on the circumstances.

Some Australian states require owners of health-related personal information to keep records of when this type of personal information is disposed of or deleted.

Access

If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information (APP 12 (Access)).

Exceptions apply, as outlined below.

An APP entity's privacy policy should include information about how an individual may access personal information about the individual that is held by the entity and seek the correction of such information (APP 1.4(d)).

An APP entity must respond to a request for access to the personal information if the entity is an agency, within 30 days after the request is made; or if the entity is an organisation, within a reasonable period after the request is made; and give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

Exceptions applicable to organisations include where:

- the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety;
- giving access would have an unreasonable impact on the privacy of other individuals;
- the request for access is frivolous or vexatious;
- the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings;
- giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations;
- giving access would be unlawful;
- denying access is required or authorised by or under an Australian law or a court order;
- the entity has reason to suspect unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities and giving access would be likely to prejudice the taking of appropriate action in relation to the matter; and
- giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

If the APP entity refuses to give access to the personal information or to give access in the manner requested by the individual, the entity must give the individual a written notice that sets out:

- the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and
- the mechanisms available to complain about the refusal; and
- any other matter prescribed by regulations made pursuant to the Act.

A sector specific access and correction framework applies in relation to credit related information.

If an APP entity holds personal information about an individual; and either the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or the individual requests the entity to correct the information, the entity must take such steps as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading (APP 13.1 (Correction)).

A breach of the APPs generally does not give rise to a cause of action exercisable at the suit of the affected individual. However, in certain circumstances the Commissioner can exercise jurisdiction and seek damages on behalf of an affected individual.

Cross-Border Disclosure and Transfer of Personal Information

Transfer of personal information is not regulated as such: the relevant act or practice that is regulated is use or disclosure of personal information. Accordingly, it is not relevant whether the custody and control of the personal information is transferred to the provider of outsourced processing services: it is sufficient if there is a disclosure, such as through the provider being provided with any form of access to the personal information.

The transfer of personal information to entities providing outsourced processing services in Australia, therefore, constitutes a disclosure of personal information for the purposes of the Privacy Act. The Privacy Act makes no distinction between disclosure of personal information to outsourced processing services and disclosure of personal information to any other third party. Each disclosure would need to be undertaken subject to the requirements of APP 6 (Use and disclosure).

APP 6 generally prohibits the disclosure of personal information by organisations unless the disclosure is consistent with the primary purpose for collection of the information, or a related secondary purpose.

However, there is an exception under the Act in relation to use or disclosures by related bodies corporate: broadly, related bodies corporate are treated as a single entity for the purposes of privacy regulation.

APP 8 also imposes restrictions on the disclosure of personal information to recipients outside Australia: these restrictions apply in addition to the disclosure restrictions under APP 6.

As is the case with disclosures to third parties within Australia, transfer of personal information to outside Australia is not regulated as such: for example, in relation to Australian regulated personal information an organisation may transfer Australian regulated personal information from its branch in Australia to another branch of itself outside Australia, or provide its overseas branch with electronic access to its Australian based database. However, in relation to any Australian regulated personal information, provision of electronic access (including read-only access) to a third party 'overseas recipient', including a related body corporate of the discloser, is a disclosure of that personal information. If the third party to whom the personal information is disclosed is outside Australia, APP 8 (Cross-border disclosure) will operate.

APP 8 does not specifically address the common scenario of provision of custody and management of encrypted Australian regulated personal information to a provider of outsourced hosting services. A sensible view is that unless there is any reasonable possibility that the provider of outsourced hosting services or persons that might reasonably be anticipated to have access to the personal information might also have the capability to decrypt and thereby at least view personal information, there is no 'disclosure' of that personal information to any overseas recipient. On this view, capability needs to be assessed 'in the round', having regard to technical capability of the provider of outsourced hosting services or persons that might reasonably be anticipated to have access to the encrypted personal information), and operational and contractual safeguards against decryption or other misuse, taken together. The Australian Privacy Commissioner's APP Guideline on APP 8 (Cross-border disclosure of personal information) at paragraph 8.14 suggests that the Privacy Commissioner will consider the provision of personal information to cloud service providers located overseas for the limited purpose of storing and ensuring that the Australian regulated entity may access that information as 'use' rather than a 'disclosure' by the Australian regulated entity if:

In practice, determining whether the provision of information to service providers constitutes a 'disclosure' or 'use' will likely be a difficult exercise and will ultimately turn on the nature of the services provided and the terms of the services agreement

- the contract with the provider requires the provider to only handle the information for these limited purposes;
- the contract with the provider requires that any sub-contractors to the provider must agree to the same obligations; and
- the contract gives the Australian entity effective control of how the personal information is handled by the overseas entity. According to the Privacy Commissioner, contractual indicators that an APP entity has retained effective control of the information include: whether the entity has retained the right or power to access, change or retrieve the personal information; who else will be able to access the personal information and for what purposes; the types of security measures that will be used for the storage and management of the personal information; and whether the personal information can be retrieved or permanently deleted by the entity when no longer required at the end of the contract.

In practice, determining whether the provision of information to service providers constitutes a 'disclosure' or 'use' will likely be a difficult exercise and will ultimately turn on the nature of the services provided and the terms of the services agreement. APP entities are expected to take a cautious approach to this issue until further clarity around the concept of 'disclosure' is provided by the Australian Privacy Commissioner or the courts.

APP 8 and section 16C of the Act also introduce an accountability approach to cross-border disclosures of personal information.

Before an organisation discloses personal information to an overseas recipient, the organisation must take reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to that information. In some circumstances an act done, or a practice engaged in, by the overseas recipient that would breach the APPs, is taken to be a breach of the APPs by the organisation. Generally, this will apply where:

- APP 8.1 applies to the disclosure (APP 8.1 applies to all cross-border disclosures of personal information, unless an exception in APP 8.2 applies); and
- the overseas recipient is not subject to the APPs, but the act or practice would be a breach of the APPs if they were.

APP 8.2 lists a number of exceptions to APP 8.1. For example, APP 8.1 will not apply where:

the organisation reasonably believes that the recipient is subject to a law or binding scheme that has the effect of protecting the information in a way that is, overall, substantially similar to the APPs; and there are mechanisms available to the individual to enforce that protection of the law or binding scheme (APP 8.2(a)); or

an individual consents to the cross-border disclosure, after the organisation expressly informs them that APP 8.1 will no longer apply if they give their consent (APP 8.2(b)).

the Australian Privacy Commissioner has not issued a list of countries whose laws, or binding privacy schemes, that the Australian Privacy Commissioner considers have the effect of protecting the information in a way that is, overall, substantially similar to the APPs and allow for appropriately effective and available enforcement mechanisms

Each of these two exceptions is difficult to interpret and apply. Attempts to invoke the exceptions are likely to be the subject of significant debate and regulatory scrutiny.

As to the former, the Australian Privacy Commissioner has not issued a list of countries whose laws, or binding privacy schemes, that the Australian Privacy Commissioner considers have the effect of protecting the information in a way that is, overall, substantially similar to the APPs and allow for appropriately effective and available enforcement mechanisms. Law firms may be expected to be unwilling to 'sign off' based upon an 'overall' assessment of laws and remedies or as to a contractual scheme, noting the difficulties of such an assessment and the exposure of the Australian entity to strict liability under section 16C in the event of any subsequent determination by the Australian Privacy Commissioner (or court enforcing a determination of the Australian Privacy Commissioner) that the foreign laws or a scheme did not in fact not qualify for the exception in APP 8.2(a). However, the Privacy Commissioner's Guidelines (at paragraph 8.21) do give some support to the use of binding corporate rules (BCRs) by international organisations, at least where the BCRs reflect "the stringent, intra-corporate global privacy policy that satisfies EU standards".

As to notice and consent, the form, prominence (conspicuousness) and level of comprehensibility of the 'express informing' are likely to be controversial. It is clear that the express notice needs to be sufficiently clear, but to ensure fully informed consent must the notice spell out what the practical effect of APP 8.1 not applying will be? The Privacy Commissioner's Guidelines (at paragraphs 8.28 to 8.30) are not prescriptive as to the form of notice, beyond stating that at the minimum the statement should explain that if the individual consents to the exposure and the overseas recipient handles the personal information in breach of the APPs, the (Australian regulated) entity will not be accountable under the Privacy Act and the individual will not be able to seek redress under the Privacy Act. Many notices as recently revised do not comply with these 'minimum' requirements. For example, consider a notice as follows (following a description of permitted purposes):

> You consent to your personal information being disclosed to a destination outside Australia for these purposes, including but not limited to the United States of America, and you acknowledge and agree that Australian Privacy Principle 8.1 will not apply to such disclosures and that we will not be required to take such steps as are reasonable in the circumstances to ensure such third parties outside of Australia comply with the Australian Privacy Principles.

The notice does not include the second limb required by the Commissioner: it does not state that the individual will not be able to seek redress under the Privacy Act. Other questions remain. How prominent does this notice need to be? If the consent is to have an ongoing operation, does the notice or consent need to be reinforced, or otherwise the subject of reminders, at periodic intervals, and if so, how often? Is the form of consent required for APP 8.2(b) different to the form of consent for other purposes, noting in this regard the unusual juxtaposition in the drafting of APP 8.2(b) of expressly informs and after being so informed, the individual consents?

APP 8.2 also introduces a number of other circumstances in which APP 8.1 will not apply:

- where the cross border disclosure is required or authorised by or under an Australian law, or a court/tribunal order (APP 8.2(c));
- where an organisation reasonably believes that the disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety (APP 8.2(d), s16A item 1);
- where an organisation reasonably believes that the disclosure is necessary to take action in relation to the suspicion of unlawful activity or misconduct of a serious nature that relates to the organisation's functions or activities (APP 8.2(d), s 16A item 2);
- where an organisation reasonably believes that the disclosure is necessary to assist any APP entity, body or person to locate a person who has been reported as missing (APP 8.2(d), s 16A item 3).

The restrictions of APP 8 apply equally to overseas transfers to service providers as to other overseas recipients. The accountability requirements of APP 8 and section 16C of the Act apply in respect of the first recipient and any subsequent recipient.

However, an act or practice engaged in outside Australia does not breach the APPs if that act or practice is required by an applicable law of a foreign country.

Credit Related Provisions

Probably the most complex changes to the Privacy Act are the credit related provisions now completely redrafted in Part IIIA of the Privacy Act (the ***CR Scheme***).

The CR Scheme applies exclusively to the collection, use and disclosure of personal credit-related information about individuals and regulates the handling of a particular type of personal credit-related information, namely credit information. Credit information comprises, on the whole, information about an individual's consumer credit history. However, credit information may also include some information about an individual's commercial credit history. One example is court proceedings information about an individual, which may relates to both commercial and consumer credit history.

The CR Scheme sets out the limited purposes for which a credit provider may use an individual's credit information. These permitted purposes include the assessment of an application for consumer credit or commercial credit (the latter only with the individual's express consent). As such, the application of the CR Scheme is not necessarily dependant on whether an individual is applying for consumer or commercial credit. Rather, the determining factor as to the

CR Scheme's application is whether a credit provider is proposing to collect, use or disclose credit information about an individual.

The majority of the restrictions in the CR Scheme address collection, use and disclosure of credit information in the course of a credit provider's engagement with a credit reporting bureau (***CRB***), such as Veda Advantage or Experian. (There are also other provisions that deal specifically with a credit provider's disclosure of information to other entities, such as debt collectors). Accordingly, if a credit provider does not collect from a CRB, or disclose to a CRB, credit information about individuals, many of the key provisions in the CR Scheme are not applicable.

The following categories of credit information are regulated under the CR Scheme.

- As noted above, the first and foundational category of information regulated by the CR Scheme is called credit information. In basic terms, credit information is essentially the personal credit-related information a credit provider collects from its dealings with an individual and discloses to a CRB. Credit information is defined exhaustively in the CR Scheme to include limited kinds of personal credit-related information, such as identification information, default information and repayment history information.
- Credit information is repackaged and consolidated with other information held by a CRB to form credit reporting information. Credit reporting information includes credit information and any information derived by CRB from the credit information. CRBs disclose credit reporting information about individuals to credit providers that request the information.
- In the hands of a credit provider, credit reporting information becomes credit eligibility information, which comprises the credit reporting information that is obtained from a CRB and any other information a credit provider derives from that information. The restrictions in the CR Scheme that govern use and disclosure of credit eligibility information by a credit provider apply only to information obtained from a CRB (and information derived therefrom) and not any other information a credit provider may have collected directly from the individual.

The CR Scheme must be read in conjunction with the terms of the Credit Reporting Privacy Code (***CR Code***). The CR Code is legally binding on credit providers and sets out further and more detailed restrictions and obligations relating to (among other things) the collection, use and disclosure of personal credit-related information.

For the purpose of determining whether an organisation is a credit provider under the CR Scheme in relation to a particular transaction, it is irrelevant whether the organisation provides a customer with consumer credit or commercial credit. This distinction only becomes relevant in relation to the purposes for which the entity may use and disclose credit information. Section 6G of the Privacy Act describes a number of scenarios in which an entity is deemed to be a credit provider. Of most general relevance, an organisation is a credit provider if it carries on a business in the course of which it provides credit in connection with the sale of goods, or the supply of services, by the supplier; and the credit is available for at least 7 days.

Emerging trends and issues

Emerging trends in Australian privacy law will reflect global trends, concerns and issues as they arise. Australia tends to closely follow major global trends, paying particular attention to regulatory developments in the U.S.A., European Union and ASEAN region.

Current trends include:

- Applications for registration and registrations of APP codes. The amendments to the Privacy Act effective from March 2014 give a prominent role to enforceable industry codes. It is expected that there will be significant industry sector activity in development of codes.
- Possible introduction of mandatory data breach notification requirements.
- Increased focus upon privacy by design and information security by design principles and practical implementation of privacy protective processes and systems by corporations.
- Review of published privacy policies for 'transparency': prominence, readability and structuring appropriate to the likely readers and as to the description of primary and secondary purposes of personal information.
- Pressure for expansion of privacy protection in relation to surveillance and geo-tracking devices and extension of the definition of personal information, or introduction of new restrictions as to 'profiling', to address concerns as to particular, perceived socially detrimental uses of big data analytics.
- Extension of privacy policy development and privacy and information security related enforcement activities by the ACMA (www.acma.gov.au), a well-resourced regulator by comparison with the Australian Privacy Commissioner.

For the purpose of determining whether an organisation is a credit provider under the CR Scheme in relation to a particular transaction, it is irrelevant whether the organisation provides a customer with consumer credit or commercial credit

- Changes to privacy regulation of news gathering and news reporting by the print and electronic media. It is likely that media codes or other media regulation affecting privacy will change in the foreseeable future.
- The ALRC's consultation and report (due June 2014) as to introduction of a statutory cause of action for serious invasion of privacy.
- Continuing pressure for more extensive regulation of third party online behavioural advertising.
- More active cross-border coordination and joint enforcement activity by the Australian Privacy Commissioner and comparable regulators in other jurisdictions.
- Continuing consultation as to alignment of privacy regulation in the Asia Pacific region.
- Focus upon law enforcement exceptions to privacy laws following the Edward Snowden revelations as to activities of the U.S. National Security Agency and national security collaboration between the 'Five Eyes' countries, including Australia.

Given the volatility and unpredictability of emergence of issues in privacy regulation, it is likely that the above list will change by addition of further issues.

Peter Leonard is a partner at Gilbert+Tobin Lawyers and a director of the International Association of Privacy Professionals ANZ (iappANZ).

Exercising Jurisdiction Over Foreign Corporations: The USA PATRIOT Act and the Extent to Which US Government Law Enforcement Agencies Can Obtain Information from Abroad

Ken Wong considers the implications of the PATRIOT Act on the ability of US Government law enforcement agencies to obtain information from abroad.

Introduction

Almost 13 years ago, the then US President George Bush signed into law the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (***PATRIOT Act***). Ever since, the PATRIOT Act has been at the centre of controversy in the international community in relation to its impact on the privacy of individuals. Prior to the signing of the PATRIOT Act, certain law enforcement and intelligence gathering legislation already had well-established extraterritorial effect. But the effect of the PATRIOT Act was to increase that extraterritorial scope. Whether data is stored within the walls of a building or in the cloud, US courts have exercised jurisdiction over foreign corporations in order to compel the production of information for the purposes of US law enforcement.

if a non-US corporation has 'continuous and systematic' contacts with a US corporation, it may be subject to US jurisdiction

The first section of this article identifies the powers which are available to US law enforcement agencies to obtain information under current US legislation. The second section highlights how the US courts have exercised jurisdiction over foreign corporations before the PATRIOT Act was signed into law. The third section is a short case note on the recent Microsoft challenge in respect of a search warrant which compelled the production of information held by its Irish subsidiary.[1] The case highlights how the US District Court applied relevant legislation after the PATRIOT Act was enacted. Finally, this article briefly discusses some considerations which may be relevant to Australian organisations when contemplating engaging with contractors and cloud computing providers.

The various methods by which US law enforcement agencies can obtain information

There are several methods available to US law enforcement agencies to obtain information from US entities and foreign companies subject to US jurisdiction. These tools were strengthened by the PATRIOT Act, which was enacted as a legal response to the terrorist attacks on 11 September 2001.[2] The PATRIOT Act amended a suite of laws relevant to law enforcement and intelligence gathering. Its preamble states that it is an 'Act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes'.[3]

Foreign Intelligence Surveillance Act (***FISA***)

FISA is the key item of legislation that was amended by the PATRIOT Act. The kinds of documents that can be obtained by the Federal Bureau of Investigation (***FBI***) are now significantly broader and include anything that is tangible as well as electronic data.[4] Recipients of a FISA order may not disclose the existence of, or the details relating to, such order.[5] One of the most significant changes was the lowering of the legal threshold for FISA orders such that the FBI need only 'specify that the records concerned are sought for an authorised investigation... to protect against international terrorism or clandestine intelligence activities'.[6] This means that a FISA order can be issued to a company which is not itself the subject of an investigation.[7]

National Security Letter (***NSL***)

NSLs enable the FBI to request various business records for the purposes of national security. An NSL is an administrative subpoena issued by the agency instead of by the court.[8] The kinds of information available to the FBI are primarily business related, which may include financial, credit, telephone and internet activity records, but content information is excluded.[9] Similar to the expansion of the scope of FISA, the PATRIOT Act also expanded the scope of NSLs. As well as imposing non-disclosure obligations, the legal threshold was also significantly reduced to only show that the information sought is relevant to a national security investigation.[10]

Grand jury subpoena

Subpoenas may be issued through *ex parte* proceedings involving a grand jury comprising a group of 16 to 23 civilian jurors to investigate the existence of possible criminal conduct .[11] Grand juries base their investigations on mere suspicion and do not follow the rules of evidence.[12] Their investigatory powers are substantial and virtually any person or document can be the subject of a grand

1 *Re Matter of a Warrant* 13 Mag. 2814 (2014).

2 Department of Justice, *The USA Patriot Act: Preserving Life and Liberty*, <http://www.justice.gov/archive/ll/highlights.htm>.

3 Department of Justice, *Text of the Patriot Act* <http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf>.

4 Patriot Act of 2001 § 215.

5 Ibid.

6 Ibid.

7 P Swire, *The System of Foreign Intelligence Surveillance Law*, 72 Geo. Wash. L . Rev. 1306, 1329 .

8 J Billings, *European Protectionism in Cloud Computing: Addressing Concerns Over the PATRIOT Act*, (2012) 21 CommLaw Conspectus 211, 216 .

9 18 USC §§ 2709 and 3414.

10 Patriot Act of 2001 § 505.

11 M Geist and M Homsi, *Outsourcing Our Privacy?: Privacy and Security in a Borderless Commercial World,* (2005) 54 UNBLJ 272, 279.

12 Ibid.

jury subpoena.[13] The PATRIOT Act amended the Federal Rules of Criminal Procedure with respect to grand juries to permit the production of documents in relation to 'matters occurring before the grand jury' involving 'foreign intelligence or counter intelligence' to 'any Federal law enforcement, intelligence, protective, immigration, national defence or national security official in order to assist the official receiving that information in the performance of his official duties'.[14]

Search warrant

Search warrants are issued by a court exercising jurisdiction over the investigation. US law enforcement agencies are required to follow the Federal Rules of Criminal Procedure and must be able to show probable cause.[15] Probable cause could be a reasonable belief that a person the subject of the investigation has committed, is committing, or is about to commit, a crime.[16] Contents of email communications and other non-content related information may be obtained by a search warrant issued under § 2703(a) of *Title 18 of the United States Code* (***18 USC***). The *Stored Communications Act* (***SCA***) was codified by 18 USC and was enacted as part of the *Electronic Communications Privacy Act of 1986*. The PATRIOT Act amended § 2703 of 18 USC to provide for nationwide service of search warrants for electronic evidence.[17]

Mutual legal assistance treaty (***MLAT***)

These are bilateral agreements under which the US Government and the foreign country to which it is a party cooperate to obtain information from each other for the investigation of crime by either country. Australia is a party to an MLAT with the US.[18]

The extraterritorially of US legislation before the PATRIOT Act

Prior to the signing of the PATRIOT Act, certain US law enforcement and intelligence gathering legislation already had well-established extraterritorial effect. This section of the article highlights how the US courts have exercised jurisdiction over foreign corporations before the PATRIOT Act was enacted.

If a foreign corporation has a connection with a US corporation, a test that the US courts have used to determine whether that foreign corporation is subject to US jurisdiction is the 'minimum contacts' test.[19] That is, if a non-US corporation has 'continuous and systematic' contacts with a US corporation, it may be subject to US jurisdiction.[20] Furthermore, when a US corporation is served with an order to produce data that is in its in possession, custody or control, and such data is held by a foreign related entity, the US courts will have regard to the closeness of the relationship between the entities to determine the level of control over the data.[21]

Where the relationship is between a US parent company and a foreign subsidiary, the US courts have considered the extent of control the US parent company has over its foreign subsidiary. The relevant test for control is whether the parent company has direct or indirect power through another company or series of companies to elect a majority of the directors of another company.[22] If the parent company has the requisite power, it will be deemed to be in control of the other company.[23]

While it is likely that a foreign subsidiary of a US parent company would be subject to US jurisdiction, there has been one case where it was held that a foreign parent company was subject to US jurisdiction. In the case of *Re Grand Jury Proceedings the Bank of Nova Scotia*,[24] which concerned the service of a grand jury subpoena on the Bank of Nova Scotia's US subsidiary branch for the production of financial information held in the Bahamas and Cayman Islands, the court held that the Canadian parent company is not excused from '[performing] a diligent search upon receipt of the trial court's order of enforcement' even if it resulted in possible breaches of local Bahamas and Cayman Island secrecy laws.[25]

Whether the services comprise data storage at a data centre or the provision of hosted software, performing due diligence on the cloud provider and understanding where the location(s) of data will be stored is vital

In another case, one US court has shown that extraterritoriality applied in the context of a tax investigation by the Internal Revenue Service. In the case of *United States v Toyota Motor Corp*,[26] summonses were issued to the Japanese parent company and to its US subsidiary. At first instance, the court found that it had personal jurisdiction over the Japanese parent company because the US subsidiary was considered a managing agent of its parent company as that term is used in the Federal Rule of Civil Procedure. The court concluded that the information sought was required to be produced because it was 'necessary for a fair and accurate determination of Toyota USA's tax liability'.[27]

Microsoft's unsuccessful challenge

With the exception of MLATs, each of the powers available to US law enforcement agencies identified above have been expanded by the PATRIOT Act. This section of the article examines how a US District Court recently applied the expanded legislation under

13 Ibid.

14 Patriot Act of 2001 § 203.

15 N Fossoul, *Does the USA Patriot Act Give U.S. Government Access to E.U. Citizens' Personal Data Stored in the Cloud in Violation of the E.U. Law?*, (2012) Paper for Tilberg University LLM Law & Technology, 14.

16 Ibid.

17 Patriot Act of 2001 § 108 .

18 *Mutual Assistance in Criminal Matters (United States of America) Regulations 1999.*

19 *International Shoe v Washington* 326 U.S. 310 (1945).

20 *Goodyear Dunlop Tires Operations, S.A. v Brown*, 131 S. Ct. 2846, 2851 (2011).

21 J Billings, above n 8, 217.

22 *In Re Investigation of World Arrangements* , 13 F.R.D 280 (D.D.C. 1952).

23 Ibid.

24 740 F.2d 817 (1984).

25 Ibid, 88.

26 569 F. Supp 1158 (C.D. Cal 1983).

27 Ibid, 5.

which a search warrant was obtained. In *Re Matter of a Warrant*,[28] the District Court of the Southern District of New York considered a motion by Microsoft Corporation (***Microsoft***) to quash a search warrant issued to it on the grounds that the US Government is not authorised to issue search warrants for extraterritorial search and seizure.

Facts

Microsoft operates and provides web-based email services under various domain names which include 'hotmail.com', 'msn.com' and 'outlook.com'. Email messages sent and received by its users are stored in Microsoft's data centres which exist in multiple locations both domestically and internationally. The location where the data is stored depends on the proximity of the user to the closest data centre.

On 4 December 2013, Francis J issued a search warrant which authorised the search and seizure of information associated with a certain email account 'stored at premises owned, maintained, controlled or operated by Microsoft'.[29] Microsoft complied with the search warrant to the extent that the relevant information was stored in servers in the US, however, it refused to comply in relation to other relevant information because it was stored in servers in Dublin, Ireland.

The relevant test for control is whether the parent company has direct or indirect power through another company or series of companies to elect a majority of the directors of another company

Microsoft subsequently filed a motion to quash the search warrant to the extent that it required the production of information that was held in Ireland.

The search warrant

The judge discussed extensively the nature and extraterritorial operation of the search warrant since the scope was expanded by the PATRIOT Act. The search warrant was obtained under § 2703(a) of 18 USC, which enables the US Government to seek from internet service providers such as Microsoft unopened emails stored by the provider for less than 180 days, as well as the kinds of information that would be available under a subpoena issued under § 2703(b) of 18 USC and under a court order issued under § 2703(d) of 18 USC.[30]

This is a very wide and powerful instrument and can compel the production of:

- basic customer information, such as the customer's name, address, internet protocol connection records, and means of payment for the account;
- content of opened emails regardless of age and content of unopened emails that are more than 180 days old; and
- historical logs showing the email addresses with which the [user] had communicated.

The judge's decision and reasoning

The judge rejected Microsoft's argument that the US Government is not authorised to issue a search warrant to the extent that it required the production of information held outside of the US. In his reasoning, the judge considered the nature of the search warrant, the legislative history of the SCA, and the practical consequences that would flow from adopting Microsoft's argument.

The judge found that the nature of the search warrant was such that it was a hybrid order which consists of part search warrant and part subpoena. Although the procedure by which it is obtained and the showing of probable cause were prerequisites to obtaining a search warrant, in terms of its execution, the order was akin to a subpoena in that it was served like a subpoena and the search and seizure of information did not require physical access to premises by US Government agents.[31] The judge's importing of the subpoena-like characteristics into the search warrant meant that the law of subpoenas applied and the recipient was required to produce the requested information which was in its possession, custody or control regardless of the location of that information.[32]

The judge also considered the legislative history of the SCA and the objectives of the relevant PATRIOT Act amendments to the SCA. Prior to the amendment, a search warrant could only be obtained in the district in which the evidence is located.[33] He considered the policy rationale underlying § 108 of the PATRIOT Act and cited that the amended § 2703(a) 'attempts to address the investigative delays caused by the cross-jurisdictional nature of the Internet... [and such] time delays could be devastating to an investigation, especially where additional criminal or terrorist acts are planned'.[34] Since the PATRIOT Act has now provided for nationwide service of search warrants, US law enforcement agencies are now able to obtain a search warrant from a court with jurisdiction over the investigation without requiring the intervention of its counterpart in the district in which the internet service provider is located.[35]

The judge also considered the practical implications that would flow if a § 2703(a) search warrant was territorially restricted. He concluded that it is unlikely that Congress intended to treat a § 2703(a) order as a conventional search warrant that involves a physical search of premises in which the evidence is located. He reasoned that a § 2703(a) order could not be a conventional search warrant because if it were, it could only be executed abroad which required the intervention of a foreign country through an MLAT.[36] The judge concluded that Congress' intention of giving § 2703(a) orders the extraterritorial reach meant that the 'slow and laborious MLAT process and the risk that the government of the other country may not prioritise the case as highly' was able to be bypassed.[37]

Microsoft is intending to appeal the decision.[38]

---

28 13 Mag. 2814 (2014).

29 Ibid, 3.

30 Ibid, 8.

31 *Re Matter of a Warrant*, above n 28, 12.

32 Ibid.

33 Ibid, 17.

34 Ibid.

35 Ibid.

36 Ibid, 21.

37 Ibid, 19.

38 Microsoft News, *Federal Judge Rules Against Microsoft In Overseas Search Warrant Case,* < http://microsoft-news.com/federal-judge-rules-against-microsoft-in-overseas-search-warrant-case/>.

Some considerations for Australian organisations

Australian organisations contemplating engaging contractors need to consider the risk of information falling into the hands of the US Government. In some cases, this could occur without their knowledge. Therefore, performing due diligence on the contractor is critical.

Before entering into an agreement with a contractor, careful consideration needs to be given to the extent to which data will be disclosed to the contractor. In particular, it is important to consider whether the data will only be held in Australia and whether there is a likelihood that data will be disclosed to an overseas entity. In a scenario where a contractor is a wholly Australian entity operating only in Australia, restricting the right of subcontracting and including a privacy clause in the contract mitigates that risk.[39] If the agreement permits subcontracting, however, it may be necessary to have the ability to approve subcontractors.[40] The level of risk will be far greater if a proposed subcontractor operates in, or has a connection with, the US.

If a contractor is an Australian entity that is part of a multinational group with a US parent company, it is likely that the Australian contractor will be subject to US jurisdicton and the risk of producing data to the US Government pursuant to an order is high. However, such risk may be somewhat reduced by preventing the flow of data to the US parent of the contractor.[41] Customers should therefore include a clause which provides for such. A useful alternative could be an obligation on the part of the contractor not to delegate any of the contracted services to any US related entity.

Australian organisations contemplating contracting with a cloud computing provider need to also consider the risks of storing data in the cloud. The risks of storing data with a non-US cloud provider that is a subsidiary of a US parent corporation is high because that provider is likely to be subject to US jurisdiction. The risks of storing data with a US cloud provider is even higher. These risks invariably raise concerns for data privacy and confidentiality for Australian organisations that have procured, or that are contemplating procuring, cloud computing services. Whether the services comprise data storage at a data centre or the provision of hosted software, performing due diligence on the cloud provider and understanding where the location(s) of data will be stored is vital. This is because the laws of the country in which the data is located is likely to have jurisdiction.

Conclusion

There is a real risk that Australian data might be the subject of a US order for production. This risk could be mitigated by ensuring that technical and contractual measures are in place before engaging with contractors or cloud computing providers. Whether a US court can exercise jurisdiction over an Australian corporation will depend on the extent of any connection with a US corporation. If an Australian corporation is a subsidiary of a US parent corporation, it is likely that a US court could exercise jurisdiction over the Australian corporation. With the rising popularity of cloud computing, the risk is exacerbated if there is a lack of control and visibility of the flow of data between data centres locally and abroad.

If an Australian corporation is a subsidiary of a US parent corporation, it is likely that a US court could exercise jurisdiction over the Australian corporation

Ken Wong is a Corporate Solicitor at Toyota Finance Australia Limited.

---

39 Treasury Board of Canada Secretariat, *Guidance Document: Taking Privacy into Account Before Making Contracting Decisions* <http://www.tbs-sct.gc.ca/atip-aiprp/tpa-pcp/tpa-pcp00-eng.asp>.

40 Ibid.

41 Ibid.

Profile: Fiona Lang
COO of BBC Worldwide Australia

In a new feature for the Communications Law Bulletin, Daniel Doctor, a member of CAMLA's young lawyers committee, chats to Fiona Lang, the new COO of BBC Worldwide Australia and New Zealand, about her new role and what she sees as the key challenges and trends in the Australian media industry.

1. You've recently been appointed to the role of Chief Operating Officer for BBC Worldwide Australia & New Zealand where did you start and how did you get to where you are?

I started out working in mergers and acquisitions at Freehills. I spent a bit of time working overseas (at Hogan Hartson & Raue, Berlin) and then returned to Gilbert + Tobin Lawyers in Sydney.

It was only very recently that I went in-house. Two years ago, I saw the Head of Legal position advertised at BBC Worldwide, and thought it would be quite a unique opportunity to get more deeply involved in media work. BBC Worldwide, is the international arm of the BBC and has a combination of public broadcasting considerations and commercial imperatives.

It is also a diverse business with an equally diverse range of legal work, including commercial, M & A, regulatory and intellectual property aspects. Our main business activities include subscription television channels on Foxtel (BBC First, UKTV, BBC Knowledge, BBC World News, CBeebies), a strong television sales distribution business and commercial brand exploitation (such as around live events, like the Doctor Who Symphonic Spectacular, consumer products and retail).

In my new role I will continue to work across the business, but will have a broader corporate advisory and strategic role in harmonising and harnessing the value of the company's activities.

2. What are the key regulatory challenges that will continue shape the media industry in Australia (and are they different at all to the challenge of doing business overseas)?

The questions of who owns our media and who is subject to the regulation of the content provided to audiences will continue to shape our industry. These are separate but related issues.

As we know, traditional media ownership is more concentrated in Australia than in many western countries which have larger populations and closer geographical proximity. Equally, media ownership restrictions here are far more extensive than many other jurisdictions. This is the subject of ongoing debate in the context of convergence, in which traditional broadcasters face increased competition from online media platforms which are not the subject of ownership laws.

Another aspect of convergence is, for example, that potentially the same content may be delivered online by an unregulated digital provider and by an Australian broadcaster to the same audience. We are yet to fully work out the appropriate regulatory implications of this for the future.

3. In recent times there has been a lot of discussion around the issues of convergence – including mooted changes to regulators and the nature of regulation . Are these still live issues for the industry and what needs to be done from a regulatory perspective to bring the law in line with the reality of media businesses today?

Yes, these are live issues and I think we will continue to see them in the legislative spotlight for some time. Convergence of media impacts upon many areas of our legal and regulatory system. Reforms to the entire framework of media legislation really need to be considered to allow issues that are relevant to the regulation of content and delivery platforms to be brought into line with the changed media environment. While this was the spirit of the Convergence Review, the scope needs to be even broader – covering areas like anti-siphoning, the use of unallocated broadcast spectrum, copyright – to ensure that not only the ways in which content is regulated across platforms, but the whole media competition landscape, is considered holistically and appropriately. Through the Federal Government's 'Deregulatory Roadmap' for Communications (just released) and statements made by the Attorney General, Brandis, around copyright and piracy, some of these broader issues are making their way to the Government's agenda.

These views have been expressed by ASTRA, the peak industry body of subscription television industry that actively represents BBC Worldwide on regulatory and policy issues impacting us.

4. If convergence was the buzz word of yesterday, perhaps 'privacy' and 'data breaches' of today, what is the issue for the media industry for tomorrow?

The 'discovery' of programming content and the associated issues relating to the surfacing of content on platforms are likely to gain increasing attention. The issue facing providers is how best to bring their content to the attention of the audience amidst the multitude of available offers and platforms. There is a need to seek solutions that go beyond the traditional media models based on offering a branded, curated offering.

We are already starting to see that broadcast and IPTV platforms are looking into set top box functionality which provides viewers with content suggestions and recommendations based on their existing viewing choices, rather than the traditional broadcast schedule programme set around primetime viewing. We are likely to see other interesting forms of disaggregation and dis-intermediation as providers seek to optimise the discovery of their content.

5. Media organisations are subject to the rules of a number of regulators (ACMA, ACCC, media codes of conduct etc). What changes would you like to see made to existing regulation?

I think changes need to be made to the regulation of competition in the media industry. We have, for example, two regulators – the ACCC, which has a clear regulatory philosophy based on enforcement and ACMA, which has a regulatory philosophy based on self-regulation, co-regulation and enforcement and codes. The ASTRA Codes which are regulated by ACMA contain provisions dealing with consumer protection that are also covered by the ACCC. Similar overlaps exist outside of the ACCC (such as in the case of privacy).

These kinds of overlaps are confusing, unnecessary and result in duplication of compliance costs.

6. What are some of the key commercial pressures that you see facing your business and this industry specifically?

The most significant commercial issue faced by the Australian media industry is the accessing of content through piracy and geo-circumvention before legal availability in Australia.

We hear much about Australia having comparatively high levels of piracy. The commercial reality is that piracy hurts the industry at every level; it undermines the investment in content for Australian audiences, which supports the employment of and reward to artists and other rights holders creating that content.

7. What are the legal risks that are unique to your industry?

Following on from the above, the biggest legal issue is the need for effective legislation that addresses illegal downloading of content in Australia. Our legislation is unfortunately lagging behind other jurisdictions in this respect, and the risks of failure to provide effective reforms are great to our industry.

8. What do you look for in effective legal advice? How do you think young lawyers can equip themselves to get closer to the business they are advising?

I look for lawyers who go beyond providing a clear legal opinion by adding additional value to my matter, such as offering insights and updates on what others in the industry are doing and suggesting creative solutions to problems.

Young lawyers should follow the developments and trends in the media and telecommunications industry and think about how these apply to their clients. Professional organisations like CAMLA and IPSANZ play such an important role in this respect!

9. What advice do you have for young lawyers wanting to work in-house ?

My advice would be to really understand and appreciate the independence required of legal counsel. When you are working in-house it is important to know and understand the business you are working for and work in a kind of partnership with the business. In that partnership, you can offer value by keeping an independent head, which permits you to challenge business decisions and work through various scenarios to get the most value from deals and protect the business from risks as much as possible.

10. What is the most enjoyable aspect about your job?

The diversity of the role and the business itself makes this a bit of a dream job for me. Our business is growing in exciting ways. For example, in August we launch our new subscription television channel 'BBC First' on Foxtel which will showcase premium scripted drama and comedy from the UK. Last year we celebrated the 50th anniversary of 'Doctor Who' with cinema screenings, exhibitions, pop-up shops and a pretty amazing Symphonic Spectacular in cities across Australia and New Zealand. Our new drama commission with the BBC (produced by RSJ Productions and See-Saw), "Banished", has recently filmed in Sydney.

I really enjoy working across the business and the most rewarding aspect is helping bring it together and watching it grow. I also love being surrounded by great BBC drama productions (produced locally or in the UK), like 'Top of the Lake', 'Luther' and 'Silk'.

Fiona Lang was recently appointed to the role of Chief Operating Officer BBC Worldwide Australia & New Zealand.

Daniel Doctor is a member of the CAMLA Young Lawyers Committee and is the Corporate Counsel at Nine Network Australia.

If you would like to suggest someone to be interviewed by the CLB, please send an email to the editors at editor@camla.org.au

The Deregulation Agenda for Australian Media Ownership: Can Competition do the Heavy Lifting?

In light of recent comments from the Communications Minister, Barry Dean, Jennifer Dean and Shyla Sharma consider the potential impact of reform of Australian media ownership regulation.

Many people have argued in recent years that the media ownership restrictions (Control Rules) in the *Broadcasting Services Act 1992* (Cth) (**BSA**) are outdated and do not reflect the current structure of the media sector.[1] The legislative intent underlying the media ownership regime has been to maintain diversity of control over the most influential media platforms.[2] There have always been "quirks" in the Control Rules.[3] However, over time, the silence of the Control Rules in relation to services provided via the internet whether it be news websites, internet protocol television (**IPTV**) or news aggregators, has in our view, lent an air of artificiality to regulatory analysis of the sector.

the silence of the Control Rules in relation to services provided via the internet whether it be news websites, internet protocol television (IPTV) or news aggregators, has in our view, lent an air of artificiality to regulatory analysis of the sector

Recent comments from the Communications Minister Malcolm Turnbull, about the need for reform have therefore struck a chord with many; but achieving a consensus on the form of any changes will be an extremely difficult task.

Although he has kept his comments relatively high level to date, the Minister has signalled his support for easing the Control Rules.[4] He has stated that, in his view, the internet is providing more avenues for competition and that, as a result, platform-specific ownership rules dealing with newspapers, radio and television are no longer required.[5] It has subsequently been reported that the Minister is leaning towards making the Australian Competition and Consumer Commission (**ACCC**) the sole referee in relation to media consolidation.[6]

At the time of writing, the government was engaged in consultation with stakeholders[7] and had indicated that it planned to publish research outlining the history of ownership controls in Australia in May.[8] The Minister has not ruled out the possibility of introducing legislation by the end of the year,[9] however, Prime Minister Tony Abbott has said he does not intend to proceed with media reform unless there is a consensus view within the industry.[10]

In this context, it is at least possible that any future reforms could result in a wholesale repeal of the Control Rules. This would leave section 50 of the *Competition and Consumer Act 2010* (Cth) (**CCA**) (which prohibits acquisitions that would, or are likely to, result in a substantial lessening of competition (SLC)) as the principal restraint upon media consolidation.

---

1 This was the underlying rationale for the previous Labor government's Convergence Review (see the Terms of Reference set out at Appendix A to the Convergence Review Final Report, March 2012). See also, Neil Hume, 'Australia's new media law irks News Corp', *The Financial Times* (online), 12 March 2013 <http://www.ft.com/intl/cms/s/0/0cf0b268-8add-11e2-b1a4-00144feabdc0.html#axzz2yoXOCfMj>; Clancy Yeates, 'Media ownership laws in firing line', *Newcastle Herald* (online), 14 December 2011<http://www.theherald.com.au/story/941696/media-ownership-laws-in-firing-line/>; Daniel Hurst, 'Malcolm Turnbull indicates easing of cross-media ownership laws' *The Guardian* (online), 9 March 2014 <http://www.theguardian.com/world/2014/mar/09/malcolm-turnbull-indicates-easing-cross-media-ownership-laws>; Michael de Percy, 'Archaic cross-media ownership laws won't save local content', *The Conversation* (online), 12 March 2014 <http://theconversation.com/archaic-cross-media-ownership-laws-wont-save-local-content-24194>; Dominic White, James Chessell and Jake Mitchell, 'Scrap cross-media ownership rules: Fairfax', *The Sydney Morning Herald* (online), 24 February 2014<http://www.smh.com.au/business/media-and-marketing/scrap-crossmedia-ownership-rules-fairfax-20140224-33chq.html>.

2 Explanatory Memorandum, *Broadcasting Services Bill 1992*, 41.

3 For example, none of subscription television services, national newspapers or public broadcasting services are taken into account in relation to the voices test under Division 5A of Part 5 of the BSA.

4 Daniel Hurst, 'Malcolm Turnbull indicates easing of cross-media ownership laws' *The Guardian* (online), 9 March 2014 <http://www.theguardian.com/world/2014/mar/09/malcolm-turnbull-indicates-easing-cross-media-ownership-laws>.

5 Ibid.

6 Darren Davidson, 'Year-end timeline to roll out dramatic media reforms', *The Australian* (online), 31 March 2014 <http://www.theaustralian.com.au/media/yearend-timeline-to-roll-out-dramatic-media-reforms/story-e6frg996-1226869244454#> and 'Turnbull questions media ownership rules', *Sky News* (online), 10 March 2014 <http://www.skynews.com.au/politics/article.aspx?id=956919>.

7 Ibid.

8 Katharine Murphy, 'Australian media regulation research to trigger fresh debate about ownership' T*he Guardian* (online), 5 May 2014 <http://www.theguardian.com/media/2014/may/05/australian-media-regulation-research-to-trigger-fresh-debate-about-ownership>

9 Darren Davidson, above n 6.

10 Katharine Murphy, above n 8.

The remainder of this article considers the recent changes in technology that are reshaping the media industry and compares the Control Rules and section 50 of the CCA in terms of their differing underlying policy rationales, operation and impact.

Changes in technology and their impact upon competitive forces in the media sector

The rate of technological change in the media sector since the ACCC released its "Media Mergers" position paper in 2006 has been remarkable. Twitter has changed how news is disseminated. The major television networks offer a significant proportion of their content on-demand online. Over 350 radio stations stream their transmissions online.[11] A consumer may access newspaper articles, live streaming of the 2UE radio broadcast, and on-demand television content including programs and movies from Fairfax Media website www.smh.com.au and news articles, live streaming of ABC radio broadcasts and on-demand ABC TV programming from the ABC website www.abc.net.au. Consumers can directly purchase and download or stream a wide variety of content online. Smart televisions and devices such as Apple TV may be used to aggregate online content on television. [12] The iPhone (from 2007), iPad (from 2010), similar mobile devices and mobile apps make the aggregation of online content even more accessible to the consumer.

There is an underlying tension here. On one hand, convergence online leads to lower barriers to entry, that is, less capital is required and there are no licensing restrictions. In addition, the product and geographic dimensions of relevant markets may be broader as a result of internet and mobile developments. These factors arguably constrain the ability of media consolidation to result in a SLC.

On the other hand, convergence may lead to established media companies having increased market power. In a converged media marketplace, media companies may need to provide audio, video and print content both online and over traditional platforms to meet consumer demands and therefore compete effectively.[13] It is a common saying in the media context that "content is king" and companies with interests in television, radio and print media may have particular advantages in the new environment because of their existing rights or capabilities to supply premium or other higher-demand news and entertainment content in different formats.

Overview of the Control Rules

The Control Rules currently prohibit a person:

- from being in a position to exercise control over commercial television broadcasting licences with a combined audience reach of more than 75% of the Australian population (**75% reach Rule**);[14] and
- from being in a position to control more than one commercial television broadcasting licence (**One-to-a-market Rule**)[15], or more than two commercial radio broadcasting licences (**Two-to-a-market Rule**) [16] in the same licence area.[17]

Any transaction that results in fewer than five independent and separately controlled voices (television, radio and newspaper) in a metropolitan radio licence area, or four in a regional radio licence area is also prohibited, unless prior approval has been obtained (**Voices Test**).[18]

the Minister has signalled his support for easing the Control Rules. He has stated that, in his view, the internet is providing more avenues for competition and that, as a result, platform-specific ownership rules dealing with newspapers, radio and television are no longer required

Finally, transactions that result in a person controlling a commercial radio broadcasting licence, a commercial television broadcasting licence and an associated newspaper in the same radio licence area without prior approval are also prohibited (**Two-out-of-three Rule**).[19]

The Control Rules vs section 50 of the CCA

The BSA is (amongst other things) supposed to:

(a) promote the availability to audiences throughout Australia of a diverse range of radio and television services offering entertainment, education and information;

(b) provide a regulatory environment that will facilitate the development of a broadcasting industry in Australia that is efficient, competitive and responsive to audience needs;

(c) encourage diversity in control of the more influential broadcasting services; and

(d) promote the availability to audiences throughout Australia of television and radio programs about matters of local significance.[20]

---

11 Australian Live Radio, <http://www.australianliveradio.com/>

12 See Wikipedia, *Smart TV* (12 April 2014) <http://en.wikipedia.org/wiki/Smart_television>; Wikipedia, *Apple TV* (10 April 2014) <http://en.wikipedia.org/wiki/Apple_tv>

13 See for example comments from Graeme Samuel as to the strategic importance of media companies owning a mix of internet, print, radio in Simon Evans, 'The future of Australian media', *Australian Financial Review* (online), 29 March 2014 <http://www.afr.com/p/national/the_future_of_australian_media_YsaRu415WuGwJFE16v13dl>

14 *Broadcasting Services Act 1992* (Cth) s 53(1).

15 Ibid s 53(2).

16 Ibid s 54.

17 There are complementary restrictions on the number of directorships a person may hold, which are consistent with the One-to-a-market and Two-to-a-market rules set out in Division 3 of Part 5 of the BSA.

18 *Broadcasting Services Act 1992* (Cth) ss 61AG, 61AH.

19 Ibid ss 61AMA, 61AMB, 61AEA. The Voices Test and the Two-out-of-three Rule speak to the position within specific commercial radio licence areas. A commercial television licence will be relevant if more than 50% of the of the radio licence area population is attributable to the licence area of the commercial television broadcasting licence (s 61AC(1) and s 61AEA(a)). A newspaper will be treated as being associated with the relevant radio licence area if the ACMA is satisfied that at least 50% of the circulation of a newspaper is within the licence area and the circulation amounts to at least 2% of the licence area population (s 59). As a result, newspapers with a national reach such as the Australian Financial Review and the Australian are not counted as voices under the Voices Test.

20 *Broadcasting Services Act 1992* (Cth) s 3.

The implicit assumption of the Control Rules is that ensuring minimum levels of diversity in ownership will promote a beneficial diversity of views across regulated platforms. This diversity is supplemented by local content requirements.[21]

The Control Rules (with the exception of the 75% reach Rule) look at individual licence areas (commercial radio and television) to ensure that certain minimum levels of diversity of control exist in relation to the regulated platforms (radio, television and print). One strength of this approach is arguably that it ensures that certain, minimum levels of diversity are protected in each licence area (to the extent that that diversity already exists). However over time, the exclusion from consideration of media that does not have a direct connection with a specific licence area has resulted in increasingly influential platforms being largely invisible from a BSA perspective and, arguably undermined the legislation's policy objectives.

companies with interests in television, radio and print media may have particular advantages in the new environment because of their existing rights or capabilities to supply premium or other higher-demand news and entertainment content in different formats

By contrast, the object of the CCA is relevantly expressed to be "to enhance the welfare of Australians through the promotion of competition". Specifically, section 50 is directed towards preventing a SLC when compared with the status quo rather than maintaining diversity above some specified minimum level.

In considering media mergers and acquisitions, the ACCC will look at markets relating to:

(a) the supply of advertising opportunities to advertisers;

(b) the supply of content to consumers; and

(c) the acquisition of content from content providers.[22]

Some markets will be national markets, but the ACCC has acknowledged that there are also local markets for some forms of advertising as well as for local content.[23]

Historically, the ACCC has tended, with some exceptions, to treat free-to-air television, radio and print media as three distinct product categories that have little overlap in terms of content or advertising markets.[24] However, as a result of technological advances (particularly in terms of the internet and mobile devices), the possibility for overlap or convergence between content and advertising across print, radio, free-to-air television, and the internet continues to increase.

The theoretical basis for section 50 of the CCA is substantially different to that of the Control Rules, not least because it is solely concerned with the levels of competition in a given market, rather than diversity of ownership *per se*. However arguably, even though the Control Rules and section 50 of the CCA are directed towards protecting different things (diversity in the case of the former and competition in the case of the latter), the practical operation of each regime may not yield results that are as different as one might expect. Moreover, to the extent that they do, this may say more about the Control Rules' focus on form and relative lack of flexibility in the face of substantial change in the industry. These propositions are explored in more detail below.

Concentration across a single platform

In a world without the One-to-a-market rule for free-to-air television or the Two-to-a-market Rule for radio, transactions that result in substantial increases in concentration may still raise section 50 issues. For example, due the limited number of free-to-air commercial television licences in a licence area and the limited number of national free-to-air television networks,[25] an acquisition that resulted in one person acquiring two of the three commercial free-to-air television stations in a licence area (potentially seeing a reduction in competitors from three to two) would appear likely to result in a SLC.

On the other hand, section 50 may not prohibit all transactions that the Two-to-a-market Rule for radio currently prohibits. A transaction that results in a person acquiring two radio stations in a single licence area is unlikely to result in a SLC except in areas with a small number of radio stations where there are distinct markets for local radio advertising and/or content. ACCC enquiries in the past have found that television advertising, television news-content and print news-content may substitute for and compete in the same market as local radio advertising and content in certain circumstances.[26]

Concentration across multiple platforms

Many transactions that would currently be prohibited under the Voices Test may also raise section 50 issues depending on the competitive constraint the lost "voice" imposes on the market. Competition issues are likely to be most acute in smaller regional areas in local advertising and news-content markets.

A hypothetical example involving Fairfax Media (**Fairfax**) and News Limited (**News**) may illustrate the extent to which SLC analysis under section 50 differs from the operation of the Two-out-of-three Rule. Since the Minister raised the review of the cross-media ownership restrictions there has been renewed speculation that News may attempt to acquire Channel Ten.[27] Because of Lachlan Murdoch's recent promotion to co-chairman of News Corp, the parent company of News, his ownership of Nova radio in Sydney, and News' ownership of the Daily Telegraph, this acquisition could not occur while the Two-out-of-three Rule remains in force (at least not without Lachlan Murdoch divesting his interest in Nova).

---

21 Local content requirements generally take the form of commercial television and radio licence conditions: sections 43A and 43C of the BSA require the ACMA to ensure that a licence conditions are in force setting out the local content obligations for commercial television and radio licences respectively.

22 ACCC, *Media Mergers* (August 2006) <http://www.accc.gov.au/system/files/Media%20Mergers%20-%202011.pdf>, 4.

23 See ACCC, *Public Competition Assessment : Macquarie Media Group – proposed acquisition of Southern Cross Broadcasting (Australia) Ltd and nine regional radio stations owned by Fairfax Media Limited* (27 November 2007) <http://registers.accc.gov.au/content/index.phtml/itemId/801331/fromItemId/751043>.

24 ACCC, above n 22, 5. However, there have been some exceptions, see for example, ACCC, above n 23.

25 See ACCC, *When three become two: Market concentration is a key factor* (13 September 2012) <http://www.accc.gov.au/media-release/when-three-become-two-market-concentration-is-a-key-factor>.

26 See ACCC, above n 23.

27 Jared Owens, 'Tony Abbott to avoid 'picking unnecessary fights' over media reform', *The Australian* (online), 10 March 2014 <http://www.theaustralian.com.au/media/tony-abbott-to-avoid-picking-unnecessary-fights-over-media-reform/story-e6frg996-1226850054378>; Bernard Keane and Glenn Dyer, 'Removal of 'two out of three' ain't bad for News Corp' *Crikey* (online), 4 February 2014 <http://www.crikey.com.au/2014/02/04/removal-of-two-out-of-three-aint-bad-for-news-corp/>

However, based on the ACCC decision to reject Seven's proposed acquisition of Consolidated Media Holdings in 2013, even if the Two-out-of-three Rule were repealed it is unlikely that the ACCC would permit News to acquire Channel Ten, Channel Nine, or Channel Seven, principally because of the opportunities that this would afford for joint bidding for premium sporting content with FOXTEL (which is 50% owned by News).[28] While in this example the outcome would be the same under both the BSA and CCA, the reasons for this are quite different and it is an open question whether, in the absence of News' subscription television interests, the transaction would be permissible from a competition perspective. A further hypothetical example illustrates this point.

The Two-out-of-three Rule currently prevents a merger between Fairfax (that controls the Sydney Morning Herald and 2UE in Sydney and The Age and 3AW in Melbourne) and Channel Ten. However, should the rule be repealed, it is less clear that such a transaction would result in a SLC. The combination would provide the merged entity with unique reach for advertising and news-content but News and other media operations would continue to exert significant competitive constraints.

Generally speaking, in regional areas, where there are likely to be fewer competitive constraints and there may be combined markets for local advertising across television, radio and newspaper platforms, it is more likely that cross-media ownership of the kind proscribed by the Two-out-of three Rule would result in a SLC.

Audience reach

Going forward, the operation of section 50 of the CCA is unlikely to restrain transactions that are currently prohibited by the 75% Reach Rule. Arguably, local content and local advertising markets would not be affected by an increased audience reach. Any potential competition issues would arise in national markets. In this context, it is difficult to see how regional free-to-air television would provide effective competition in national markets against Channel 7, Channel 9 or Channel 10. Any repeal of the 75% reach Rule is likely to result in a series of mergers between the national networks and their regional affiliates. Indeed, a number of such transactions have already been canvassed in the press.[29] However, given the substantial overlap of content between the major networks and their regional affiliates, it is hard to see how this would result in any significant detriment to competition or diversity.

Conclusion

If the current government's media ownership reform agenda results in the repeal of the Control Rules, how might the media landscape change? It seems likely to us that a certain amount of consolidation that would be currently prohibited under the BSA might be permitted, especially:

(a) in capital cities (or other well serviced areas) where high levels of competition (and diversity) exist; and/or

(b) between the major television networks and their regional affiliates.

The great unknown at present is the extent to which internet-based services such as those offering streaming and on demand television and radio content and news aggregation will become substitutes for traditional print, radio and television services or the extent that this will result in less concentrated media markets

In our view, such consolidation is unlikely to have a significant affect upon media diversity (except in a purely formalistic sense). Conversely, areas that are less well served are more likely to be protected from further substantial consolidation, by the ACCC's focus on the markets for local content and advertising.

The great unknown at present is the extent to which internet-based services such as those offering streaming and on demand television and radio content and news aggregation will become substitutes for traditional print, radio and television services or the extent that this will result in less concentrated media markets.

The ACCC has accepted that internet-based services are relevant to the competition analysis in relation to television content and advertising and that they may operate as a competitive constraint.[30] However, this argument still has some way to run. Moreover, given the ACCC's willingness to consider the markets for the acquisition and supply of local content services,[31] convergence, and the availability of national and international content online may not necessarily result in substantially more mergers of media operations in the same local markets, especially where those markets are in regional areas.

Barry Dean is a Barrister on 5 Wentworth, Jennifer Dean is a senior associate and Shyla Sharma is a Graduate at Corrs Chambers Westgarth.

---

28 ACCC, *Public Competition Assessment: Seven Group Holdings Limited – proposed acquisition of remaining shares in Consolidated Media Holdings Limited* (15 February 2013) <http://registers.accc.gov.au/content/index.phtml/itemId/1084318> where at p 8-10 the ACCC concluded that due to ability to influence Fox Sports Australia or FOXTEL and the importance of premium sports to free to air television the acquisition would substantially lessen competition in the free-to-air market.

29 Madeleine Heffernan, 'John Singleton eyes Prime Media after board departure' *Sydney Morning Herald* (online), 3 March 2014<http://www.smh.com.au/business/john-singleton-eyes-prime-media-after-board-departure-20140302-33ty9.html>; Jared Owens, above n 27; David Crowe, 'Malcolm Turnbull faces media reform fight', *The Australian* (online), 10 March 2014 <http://www.theaustralian.com.au/media/malcolm-turnbull-faces-media-reform-fight/story-e6frg996-1226849779831#>

30 ACCC, *Public Competition Assessment: FOXTEL - proposed acquisition of Austar United Communications Limited* (14 June 2012) <http://registers.accc.gov.au/content/index.phtml/itemId/1044881/fromItemId/751043>

31 For example, ACCC, above n 23; ACCC, *Public Competition Assessment: Fairfax Media Limited – proposed acquisition of Southern Independent Publishers Ltd's Kiama Independent and Lake Times newspapers* (3 May 2011) <http://registers.accc.gov.au/content/index.phtml/itemId/961950/fromItemId/751043>

Communications & Media Law Association Incorporated

The Communications and Media Law Association (**CAMLA**) brings together a wide range of people interested in law and policy relating to communications and the media. CAMLA includes lawyers, journalists, broadcasters, members of the telecommunications industry, politicians, publishers, academics and public servants.

Issues of interest to CAMLA members include:

- defamation
- broadcasting
- copyright
- advertising
- information technology
- freedom of information
- contempt
- privacy
- censorship
- film law
- telecommunications
- the Internet & on-line services

In order to debate and discuss these issues CAMLA organises a range of seminars and lunches featuring speakers prominent in communications and media law policy.

Speakers have included Ministers, Attorneys-General, members and staff of communications regulatory authorities, senior public servants, executives in the communications industry, lawyers specialising in media and communications law, and overseas experts.

CAMLA provides a useful way to establish informal contacts with other people working in the business of communications and media. It is strongly independent, and includes people with diverse political and professional connections. To join CAMLA, or to subscribe to the Communications Law Bulletin, complete the form below and forward it to CAMLA.

Disclaimer

The Communications Law Bulletin is the journal of the Communications and Media Law Association (**CAMLA**) which is an independent organisation which acts as a forum for debate and discussion and welcomes the widest range of views. The views expressed in the Communications Law Bulletin and at CAMLA functions are personal views of the respective authors or speakers. They are not intended to be relied upon as, or to take the place of, legal advice.

Contributions & Comments

Contibutions and Comments are sought from the members and non-members of CAMLA, including features, articles, and case notes. Suggestions and comments on the content and format of the Communications Law Bulletin are also welcomed.

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

Valeska Bloch or Victoria Wark
C/- Allens
Deutsche Bank Place
Corner Hunter & Philip Streets
SYDNEY NSW 2000

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

CAMLA contact details:

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

CAMLA Website

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

Application for Membership

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

Name:.....

Address: .....

Telephone: .....Fax: .....Email: .....

Principal areas of interest: .....

.....

I hereby apply for the category of membership ticked below, which includes a Communications Law Bulletin subscription, and enclose a cheque in favour of CAMLA for the annual fee indicated:

☐ I Ordinary membership $130.00 (includes GST)

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

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

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