Communications Law BULLETIN

CAMLA

Communications & Media Law Association Incorporated

Print Post Approved PP: 234093/00011

For Your Information

Hamish Fraser covers the recently released ALRC Report on Privacy.

For Your Information: Australian Privacy Law and Practice is the title of the Australian Law Reform Commission's (***ALRC***) long awaited report on Australia's Privacy Laws tabled in Federal Parliament on 11 August 2008.[1]

By any measure the ALRC's report and the work that has gone into it is big. It is 2700 pages long with 74 chapters and 295 recommendations, and by all accounts if you print it all out, it will come in at over 5kg. The original reference was made over two and a half years ago and under a different Government.

More importantly the ALRC undertook an enormous volume of work to complete this report, including 585 written submissions, three major public forums, over 200 hundred face to face meetings, roundtables with stakeholders, and a two day phone in, with over 1000 members of the public calling the ALRC to share their opinions.

So perhaps it's a good thing that Senator Faulkner has indicated it is likely to be 18 months before any of the recommendations are implemented and the more controversial recommendations (including the statutory action for invasion of privacy and removal of exemptions) have not been given any specific timeline for review. We will all have plenty of time to get ourselves comfortable with what the new regime is going to look like.

The Parts We Expected

There are, as most observers will have expected, a number of recommendations that are not surprising.

Perhaps highest on the agenda (and in fact the first of the recommendations) is the acknowledgement of the need for a nationally consistent set of rules for the handling of personal information by organisations, removing, amongst other things, the overlap with the various state legislation, in particular the state health records laws.

A consistent set of Privacy Principles (the ALRC refers to them as the Unified Privacy Principles) is another recommendation that many will have expected, as well as recommendations to remove many of the exemptions from the existing legislation (employee record, small business and political party). Interestingly the ALRC observed that whilst some tightening is required, the journalism exemption should be retained.

Another of the 'not surprising' bundle of recommendations is an acknowledgement of the need for improvement of the credit reporting framework.

The Current Law and Technological Developments

One of the benefits of the work undertaken by the ALRC is the opportunity it gave them to review and comment on the operation of the current privacy framework plus the recent judicial and scholarly commentary on the concept of privacy, and then to use that to inform its recommendations. Whilst too lengthy to restate here, their analysis suggests that definitions are problematic, and a pragmatic approach to law reform is favourable, such that:

> *Rather than focusing on an overarching definition of privacy, it makes more sense,…to focus on particular points in the web and formulate a workable approach to deal with the disruption.*[2]

The current privacy legislation was largely the result of the recommendations of the ALRC in 1983, then chaired by one of Australia's most influential jurists, Justice Michael Kirby. That too was an extensive inquiry and, at a time before Bill Gates was a household name, was far sighted enough to identify that technology represented one of the chief threats to privacy.

Consistent with the onward march in technology, high on the list in this report are recommendations regarding the need to

Volume 27 N° 1
August 2008

Inside This Issue:

Communications Law Bulletin

Editors: Matt Vitins, Page Henty & Lesley Hitchens

Printing & Distribution: BEE Printmail

Website: www.camla.org.au

Contents

accommodate developments in technology. These are aimed at empowering the Privacy Commissioner to consider, use and publish materials on privacy-enhancing technology and those that may impact upon privacy.

Other Recommendations

Recommendations 71 and 72 call for a number of changes to the *Telecommunications Act 1997* (Cth), including a prohibition on charging a fee to keep a telephone number unlisted and that the use and disclosure provisions be redrafted to achieve a clearer and simpler regime.

The recommendation attracting perhaps the most public interest is the suggestion that there will be a cause of action for a 'serious invasion of privacy'.[3] Whilst this is one of the areas the Government has not committed to a legislative timeframe, the ALRC suggests that to establish liability, a claimant must show that:

a) there is a reasonable expectation of privacy; and

b) the act complained of is highly offensive to a reasonable person of ordinary sensibilities.

In determining whether the cause of action is made out, the ALRC acknowledged that a court would have to take into account the balance between the individual's privacy and the public interest.

Other recommendations contained in the report are:

- Stronger penalties are recommended[4] to enable the Privacy Commissioner to seek civil penalties for serious interference with the privacy of an individual;
- Empowering privacy beyond the individual[5] – namely making recommendations to address the privacy needs of Indigenous groups;
- Privacy of deceased people[6] - recommending amendments to the Privacy Act to protect certain information relating to persons who have been dead for less that 30 years; and
- A restructure and 'beefing' up of the office and the powers of the Privacy Commissioner.[7]

Hamish Fraser is a Partner at Truman Hoyle Lawyers in Sydney

(Endnotes)

1 http://www.austlii.edu.au/au/other/alrc/publications/reports/108/

2 Ibid at 1.67

3 Recommendation 74

4 Recommendation 50

5 Recommendations 7-1 and 7-2

6 Recommendation 8

7 Recommendation 47

When Worlds Collide – Indefeasible Rights of Use, Tax and Commercial Reality

James Halliday and Linh Tran discuss the nature and form of Indefeasible Rights of Use agreements as a distinct type of capacity supply arrangement that can have tax advantages.

Introduction

In 1951, Paramount Pictures released the blockbuster hit, *When Worlds Collide*. It told of the cataclysmic results of two rogue planets from outer space crashing into Earth, pulverizing the planet and all life on it. The collision of several worlds is a good way to describe the process of drafting an 'Indefeasible Right of Use' (***IRU***) agreement. This process involves the collision of commercial, accounting and tax requirements in a way that requires a very strong understanding of each in order to be reconciled in a workable agreement.

Jumping forward from 1951 to 2008, it is interesting to see that there have been a number of recent announcements regarding the deployment of international submarine cable commission and upgrade projects over the next 18 months.[1] The anticipated growth in the availability of quality high speed transmission capacity is likely to see an increase in commercial arrangements for capacity supply. This is relevant not only to traditional telecommunications infrastructure companies, but also very important to other industry participants such as media and content providers, who are expected to exploit their applications using the capacity on these cables.

When negotiating these capacity supply arrangements, the parties will undoubtedly consider the various forms of arrangement that are available. In this article we look at what constitutes an IRU arrangement as distinct from other capacity supply arrangements, the key drivers underlying these arrangements and the tax and commercial requirements that are typically important to the contracting parties. It also offers some suggestions as to how best to manage the often competing requirements in the modern environment.

Why an IRU?

'Normal' capacity supply arrangements

Participants in the telecommunications industry will be familiar with the 'normal' forms of capacity supply arrangements. The contracts which document these arrangements usually describe the capacity to be supplied, the price to be paid, limitations of liability of the supplier, and the rights of the supplier to stop supplying the capacity in the event of the customer's default (e.g. non-payment).

A 'normal' capacity supply arrangement will typically have the characteristics shown in Figure 1.

IRUs distinguished

An IRU, in a telecommunications context, is a form of capacity supply arrangement which, as will be seen, exhibits characteristics quite different to those of the 'normal' supply arrangements described above. In telecommunications slang, an 'IRU' generally refers to a long-term arrangement (e.g. for a term of 10 to 15 years) under which a supplier grants its customer rights to capacity over a fibre optic cable system.[2] Often the arrangement requires the customer to make an upfront lump sum payment to the supplier to have these rights for the life of the agreement.

The term 'IRU' also has a specific and narrow meaning under the *Income Tax Assessment Act 1997* (Cth).[3] One consequence of a particular arrangement falling within this narrow meaning is that both the supplier and the customer are entitled to treat the arrangement as capital in nature.[4] This means, for example, that the customer is able to obtain certain tax depreciation allowances that might not otherwise be possible in connection with a normal supply arrangement – that is, payments for the capacity by the customer are treated as capital payments and are therefore depreciable over the life of the relevant cable (this can often translate to significant tax savings for the customer).

Importantly, the essence of an IRU arrangement is the conferral of economic (but not legal) ownership of the capacity, and/or cable over which the capacity is carried, to the customer. This means that IRU agreements typically require the customer to take the risk of damage to the cable system, even though this is generally not within their control. On the other hand, IRU agreements usually also allow the customer to use the relevant capacity on the same terms and conditions as the supplier.

Figure 1

Supplier	→	Customer
(obligation to supply)		(obligation to pay)
(service is rarely over a fixed or agreed route)		(service is rarely supplied exclusively to customer)
(can terminate for default by customer)		(can terminate for failure to supply service)
(must maintain service to agreed level)		(can claim service credit or other damages for failure to supply)

Figure 2

Supplier	→	Customer
(grants indefeasible right to use)		(obtains indefeasible right to use on same terms as supplier)
(service must be supplied over a fixed route)		(service is supplied exclusively to customer)
(cannot usually terminate for failure to pay)		(cannot usually terminate for failure to supply)
(not required to maintain service)		(cannot claim service credit or other refund from supplier)

An IRU agreement will typically have the characteristics shown in Figure 2.

Key indicia of IRUs

Overview

There are no criteria which definitively distinguish IRUs from other capacity supply arrangements. When seeking to determine whether a particular arrangement is an IRU (at least for tax purposes), each arrangement is considered on a case by case basis. Broadly, however, there are two essential indicators which, if reflected in the terms of the supply arrangement, assist its characterisation as an IRU. These features are:

a) indefeasibility; and

b) the customer's right to use the capacity on more or less the same terms as the owner.

Both indicators stem from the idea that, under an IRU arrangement, economic ownership of the relevant capacity/cable is conferred to the customer. It is therefore helpful when approaching IRU agreements to think of an IRU as giving effect to the transfer of a tangible asset, such as a car, and thinking about how certain situations might be dealt with if the agreement were for the sale and purchase of that asset rather than for the supply of a service.

The following sections describe how capacity supply arrangements are often structured, and the provisions often included, so as to reflect the above indicators. Generally speaking, the greater the number of these provisions in an agreement, the more likely it is that the arrangement will be regarded as an IRU.

Indefeasibility

The first key indicator of an IRU is that it is indefeasible. In order to be indefeasible, it is usually necessary that the relevant capacity is:

- **Identifiable.** If a supplier sells a tangible physical asset to a customer (e.g. a car), then the asset must obviously be identified and known. In the case of an IRU, the arrangement should ideally be for capacity over specific wavelengths within a specific fibre strand, or over specific fibre strands within a specific cable, or at the very least, over a specific route or routes.
- **Fixed.** As part of the requirement that the asset be identifiable, the amount of capacity must also be fixed.
- **For the customer's exclusive use.** If a person owns a car, they usually have the exclusive right to use that car. Similarly, the capacity or infrastructure must be exclusively made available to the customer, and not shared with any third person.

To evidence indefeasibility, IRU agreements typically:

- do **not** include a right to terminate by either party; and
- do **not** allow for the customer to receive refunds of any payments made upfront for the capacity.

Rights more or less similar to that of the owner

The second key indicator of an IRU is that the customer must have a right to use the capacity on the same terms, more or less, as those on which the owner is entitled to use that capacity.

To reflect this idea of quasi-ownership, IRU agreements typically contain the following types of clauses:

- **No obligation to maintain**. The purchaser of a car has the entire obligation to service that car. Similarly for an IRU, the supplier cannot have an obligation to maintain the cable system or relevant service to any particular level.[5]
- **No compensation for defective service.** Unless there is a separate warranty arrangement, the purchaser of a car has no general law right to receive compensation if the car breaks down. Similarly, the customer in an IRU arrangement is not entitled to receive any kind of compensation (such as service credits or rebates) if the cable system fails or otherwise becomes inoperative, or for interruption to the supply of capacity.
- **Customer must meet share of the costs of uninstalling the cable system**. The purchaser of a car must meet the cost of disposing of it when it reaches the end of its life. Similarly, the customer in an IRU arrangement must contribute its proportional share of the cost of uninstalling the cable system, if the cable system is liquidated.
- **Customer receives share of proceeds of disposal.** The customer in an IRU arrangement is entitled to a proportional share of any proceeds which arise from the installation of the cable system or from claims against third parties in respect of it.

Again, because of this indicator, the agreement will generally not include a right for the customer to terminate the agreement, even where there is failure by the supplier to make the relevant capacity available.

Drafting IRU Agreements for Typical Commercial Arrangements

Perhaps not surprisingly, the indicators of IRU agreements and the ideal 'IRU provisions' rarely match the actual commercial requirements of the parties to them. For example, customers of telecommunications services usually expect to have the right to terminate the services arrangement where the supplier fails to supply that service. As discussed, this is not usually permitted in a true IRU agreement. Similarly, customers do not typically expect to have to meet the cost of repairing cable cuts, as this is usually the obligation of the supplier.

The key challenge with IRU agreements is, therefore, to structure the arrangement so that it incorporates the key IRU indicators, but still meets the commercial requirements of the parties. This section looks at some of the ways in which this might be achieved. Some of these requirements go purely to form,[6] whereas others go to substance.

Where there are strong tax objectives driving the IRU arrangement, it is important that the parties be mindful of the anti-avoidance provisions of applicable tax legislation and ensure that they structure the arrangement in a manner that does not contravene any relevant prohibitions. Specialist tax advice should obviously be sought in such circumstances.

Operations and maintenance services

Under a normal capacity supply arrangement, the customer will usually want the service to be supplied to a certain standard or 'service level' (for example, the supplier may promise to supply the service to a certain availability target). The customer will usually also ask for some kind of liquidated damages or 'service credit' if the service is not provided to the contracted level.

An IRU arrangement, however, requires the customer to take on the risks and benefits of ownership of the cable system. Theoretically, this means that the customer must also take on the obligation to maintain that system. Accordingly, a requirement that the supplier satisfy defined service level requirements cannot (strictly speaking) form part of an IRU agreement. This is potentially problematic in that, as a matter of practice, it is rarely feasible for the customer to assume the cable operations and maintenance obligations itself.

This issue is typically resolved by the customer outsourcing operations and maintenance obligations back to the supplier. Thus, an IRU agreement is usually accompanied by a separate operations and maintenance agreement which governs the provision of these services.

A further and related complexity is that, because the customer (theoretically) must bear risks in respect of the cable (or relevant part), such as the risk of damage and obsolescence, the customer should bear its proportion of the costs of repairs and upgrades of the cable. Commercially, however, the customer may be unwilling to pay additional amounts to the supplier in the event of damage to the cable or other circumstances which require the cable to be upgraded.

One way to address this issue could be to include a provision in the operations and maintenance agreement which requires the supplier to indemnify the customer for any repair and upgrade costs in consideration of the customer paying a specified premium. The premium would then be drafted as being an amount that is included in the total IRU fees under the IRU agreement so that the customer would not, in practice, pay any additional amounts to the supplier.

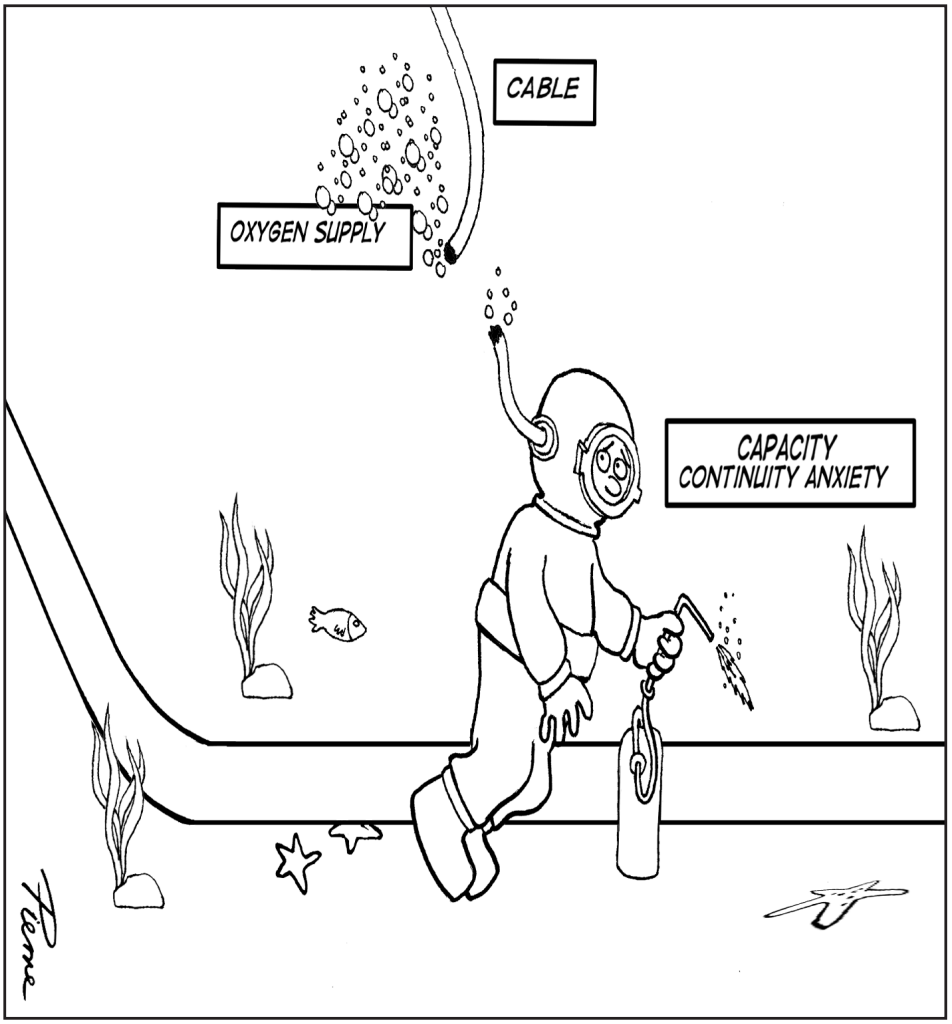
Flexibility of capacity requirements

As discussed above, the requirement of indefeasibility generally means that the IRU agreement needs to identify the relevant capacity, ideally, by identifying specific fibre strands or routes. In some cases, however, it is not always desirable or even possible to include these details at the time of entering into the agreement. In other cases, the parties may simply wish to preserve some flexibility as to the capacity over which they have rights during the term of the arrangement.

Of course, to expressly include a right for either party to specify the fibre strands or routes at a later time, or to change those fibre strands or routes during the term, would be inconsistent with the idea of an IRU being a defined asset. Indeed, the inclusion of such rights would quite clearly make the arrangement one for the supply of services.

In these situations, the agreement should be drafted to include as much detail as possible in respect of the capacity requirements that are not expected to change over the term of the arrangement. It should then also include provisions which allow flexibility for the other requirements to change as necessary during the term. Some examples of how this might be done in different scenarios are as follows:

- A customer will generally require continuity of capacity supply notwithstanding faults affecting the relevant fibre strands. To ensure this is possible, the agreement should allow for the customer to exercise its rights of use in relation to capacity on alternative fibre strands where there is a fault on the specific fibre strands over which the customer normally obtains the capacity, until the fault is remedied. In this scenario, it might be sufficient to simply identify the amount of capacity to be supplied and the cable over which it is to be supplied. This would mean that in the event that the supplier needs to provide the customer with capacity over fibre strands that are different to those contemplated at the commencement of the arrangement, it is able to do so and still be within the terms of the agreement.
- A customer may require the capacity on different routes during the term to accommodate its changing business needs and the demands of its own customers. This scenario can be accommodated to some extent by specifying upfront the fixed capacity requirements (which are likely to be the aggregate amount of required capacity, and the possible routes over which that capacity may be required), and including a provision stating that the IRU is to be activated progressively in accordance with the terms of a separate agreement (e.g. the operations and maintenance agreement). That other agreement would then include a mechanism under which the customer can, from time to time, direct activation of rights to capacity over the various routes specified in the IRU agreement.
- A supplier, while able to undertake to provide an IRU for capacity between specified points, might not be able to specify the fibre strands, or even the routes, over which rights to capacity will be granted because the relevant cables are not yet built. In this scenario, it would only be possible to specify the aggregate amount of capacity required and the physical locations between which the capacity is required. The flexibility would need to be built in by way of a provision stating that the IRU is granted for the specified amounts of capacity between the specified locations along routes which are to be determined pursuant to a design process. The design process would then need to be set out in a separate agreement (typically referred to as a 'design and construct' agreement).



Termination rights

It is reasonable, and usual, for a customer to expect a right to terminate a capacity supply arrangement where the supplier fails to provide the relevant capacity. The customer might also expect a right to a refund of any amounts paid upfront for that capacity. Similarly, it is usual and reasonable for a supplier to expect a right to terminate the arrangement where the customer defaults in payment. As discussed above, however, a true IRU agreement generally cannot be terminated and cannot allow for refunds of upfront payments.

One way to consider in which the potential inequities arising from these restrictions can be overcome is by incorporating put and call options in the IRU agreement which would apply in the event of the supplier's and customer's default, respectively. These might work as follows:

- Under the put option, the customer would be entitled to 'put' its interest in the IRU to the supplier in the event of the supplier's breach (e.g. failure to provide the capacity). Upon exercise of the put option, the supplier would be required to purchase that interest for a specified amount – for example, the amount paid by the customer for the IRU. This would effectively result in a refund of the amount paid by the customer to the supplier.
- Under the call option, the supplier would be entitled to 'call' its interest in the IRU in the event of the customer's breach (e.g. failure to pay for the capacity). Upon exercise of the call option, the customer would be obliged to sell that interest back to the supplier for a specified amount – for example, the amount

owed by the customer. This would effectively cancel out the amount owed by the customer to the supplier.

The operation of either the put option or call option would effectively result in the capacity supply arrangement coming to an end, consistent with the commercial intention to allow for termination in the event of default. Given the values involved, the options should be drafted such that they can only be exercised following a significant and comprehensive dispute resolution process, similar to what would apply in connection with termination rights under a services agreement.

Conclusions

As seen from the examples in this article, the commercial requirements of parties to capacity supply arrangements typically do not match the strictures of a true IRU. The means of addressing this dichotomy will depend on the specific arrangement, as the commercial and other objectives will invariably differ in each case. Considerable legal ingenuity incorporating tax, accounting and other advice (as appropriate) is therefore often required to produce an agreement that is reflective of the commercial intent of the parties but which also complies with the requirements of the IRU and its inherent complexities. There are potentially significant benefits to be had by both the supplier and customer (such as tax and accounting effectiveness) where the parties manage to steer a successful collision of the various objectives underlying an IRU arrangement which often travel in different directions.

James Halliday is a Partner and Linh Tran an Associate at Baker & McKenzie in Sydney.

(Endnotes)

1 For example, Telstra and Alcatel-Lucent are currently constructing a Sydney-Hawaii cable; Pipe Networks has recently announced a second cable to New Zealand; and upgrades have recently been completed on the Australia-Japan Cable.

2 It may be possible to structure arrangements for the supply of capacity over other fixed transmission technologies, such as microwave and satellite, as IRUs. However, such 'IRUs' are unlikely to constitute IRUs for tax purposes.

3 The *Income Tax Assessment Act 1997* (Cth) defines an 'IRU' as 'an indefeasible right to use a telecommunications cable system' in section 995.1.

4 IRUs can in some cases also amount to 'finance leases' or 'sales type' leases for accounting purposes. A finance or sales lease is also regarded for accounting purposes as a capital asset. In some cases this can mean that the supplier is entitled to account for the entire upfront payment as revenue in the financial year in which it is received. This article does not examine the accounting treatment in detail of IRUs.

5 This is mitigated through the use of operations and maintenance agreements, described below.

6 For example, most capacity supply arrangements will, in practice, entail the supplier providing services (i.e. the supply of capacity) to the customer. Notwithstanding this, if the arrangement is to be characterised as an IRU, it must be drafted in a way that does not imply a services arrangement. At the most basic level, this means that the IRU agreement should not refer to the 'supply' or 'delivery' of capacity or services, or any words or obligations to that effect. Instead, these agreements typically refer to the 'grant of an IRU', implying a once-off, upfront provision of an asset (e.g. under a sale agreement), as opposed to an ongoing services arrangement.

The Producer Offset – A Shot in the Arm for Australian Film

Nick Abrahams and Victoria Dunn review available tax incentives designed to support the Australian screen media industry.

The recently introduced 40% producer offset for feature films has been a big success for at least one Australian production with Animal Logic's $100 Million *Guardians of Ga 'Hoole* receiving interim approval for the offset.

The *Tax Laws Amendment (2007 Measures No. 5) Act 2007* (Cth) amended the *Income Tax Assessment Act 1997* (Cth) (the ***Act***) by introducing three tax incentives to support the Australian screen media industry. Those incentives take the form of refundable tax offsets designed to encourage private sector investment in the Australian screen media industry. The three tax incentives are the producer offset, the location offset and the PDV (post, digital and visual effects) offset. The three offsets replaced the tax incentives for films available under Division 10BA of the *Income Tax Assessment Act 1936* (Cth). A company is entitled to only one of those offsets in relation to a film.

The producer offset is a considerable financial incentive available to producers of films, amounting to 40% of a company's qualifying Australian production expenditure for feature films and 20% of production expenditure for films which are not feature films. A feature film is a film of at least one hour in length that is screened as the main attraction in commercial cinemas.

Eligibility

A company is entitled to claim the producer offset in its tax return for an income year in respect of a film completed in that year if the company

- satisfies certain residency requirements; and
- holds a certificate for the producer offset for the film.

A company is not entitled to the producer offset if:

- the company or someone else claims a deduction in relation to a unit of industrial property that relates to copyright in the film under Division 10B of Part III of the *Income Tax Assessment Act 1936* (Cth);
- a final certificate for the film has been issued at any time under Division 10BA of Part III of the *Income Tax Assessment Act 1936* (Cth);
- a certificate for the location offset or PDV offset has been issued for the film at any time;
- the company or someone else has deducted money paid for shares in a film licensed investment company which has invested in the film; or
- production assistance (other than development assistance) for the film has been received by the company or anyone else before 1 July 2007 from the Film Finance Corporation Australia Limited, Film Australia Limited, the Australian Film Commission or the Australian Film, Television and Radio School.

Key requirements for issue of a certificate for the producer offset

The Film Finance Corporation Australia Limited (***FFC***) is currently responsible for the issuing of certificates for the producer offset. However, the *Screen Australia and the National Film and Sound Archive (Consequential and Transitional Provisions) Act 2008* (Cth) enacted 20 March 2008 provided that this function of the FFC would be assumed by Screen Australia on 21 August 2008.

The key requirements for the issue of a certificate for the producer offset for a film are:

- the film has significant Australian content or has been made under an arrangement between the Commonwealth and a foreign country; and

- the total of the company's qualifying Australian production expenditure on the film is above the minimum set amount.

Significant Australian content

In determining whether a film has a significant Australian content, the FFC (or Screen Australia) must have regard to:

- the subject matter of the film;
- the place where the film was made;
- the nationalities and places of residence of the persons who took part in the making of the film;
- the details of the production expenditure incurred in respect of the film; and
- any other matters that the film authority considers to be relevant.

Further criteria apply for a film that is a series.

Qualifying Australian production expenditure

The producer offset is only available where the qualifying Australian production expenditure on a film is above a set minimum amount. The minimum amount varies with the format of the film. In respect of feature films the minimum expenditure threshold is $1 million.

A company's qualifying Australian production expenditure on a film is the company's production expenditure on the film to the extent to which it is incurred for, or is reasonably attributable to:

- goods and services provided in Australia;
- the use of land located in Australia; or
- the use of goods that are located in Australia at the time they are used in the making of the film.

It is the FFC's (or Screen Australia's) responsibility to determine a company's qualifying Australian production expenditure on a film for the purposes of the producer offset.

Subdivision 376-C of the Act sets out how a film's qualifying Australian production expenditure is to be calculated.

Other requirements for issue of a certificate for the producer offset

In addition to having significant Australian content and sufficient qualifying Australian production expenditure, the following requirement must also be met before a certificate for the producer offset can be issued:

- the applicant company must have either carried out, or made the arrangements for the carrying out of, all the activities that were necessary for the making of the film;
- the film was produced for exhibition or distribution to the public;
- the film is of a particular type, including a feature film, single-episode programme, series, season of a series or a short-form animation; and
- the film is not an advertising program or a commercial, a discussion program, a quiz program, a panel program, a variety program or a program of a like nature, a film of a public event (other than a documentary), a training film, a computer game, a news or current affairs program or a reality program (other than a documentary).

Refusal to issue a certificate for the producer's offset

If the FFC (or Screen Australia) refuses to issue a certificate for the producer offset for a film, it must give the applicant written notice of the decision, including reasons for the decision.

The notice must contain a statement to the effect that an application may be made to the Administrative Appeals Tribunal (the ***AAT***) by, or on behalf of, any entity whose interests are affected by the decision, for review of the decision.

The notice must also include a statement to the effect that an applicant may request a statement setting out the findings on material questions of fact, referring to the evidence or other material on which those findings were based and giving the reasons for the decision or determination.

However, a failure of the FFC (or Screen Australia) to comply with those requirements will not affect the validity of the decision.

Notices issued by the FFC are not available publicly.

Procedures for review of the FFC's (or Screen Australia's) decisions

The Act expressly provides for review by the AAT of a decision of the FFC (or Screen Australia) to refuse an application for a certificate for the producer offset.

At time of writing, the AAT has not yet considered any decision of the FFC in relation to the producer offset. Although the AAT has reviewed decisions in respect of certificates issued under the superseded Division 10BA incentives for films, those decision relate to the application of the certificates, rather than to the issue of a certificate itself. There is therefore little guidance as to the approach the AAT would take to the key concepts of significant Australian content and qualifying Australian production expenditure.

Conclusion

The producer offset has the potential to act as a significant incentive to companies to invest in the Australian screen media industry. It is hoped that Screen Australia's assumption of responsibility for issuing certificates for the producer offset in 2008 will bring with it increased guidance to companies as to how the requirements set out in the Act are applied.

Nick Abrahams is a Partner and Sydney Chairman and Victoria Dunn a Lawyer at Deacons in Sydney

Degrees of Influence

Heidi Bruce considers the continued relevance of the 'degree of influence' principle as a regulatory philosophy of the Broadcasting Services Act.

Introduction

The foundation principle underpinning the regulatory framework of the *Broadcasting Services Act 1992* (Cth) (***BSA***) was the intention that different levels of regulatory control should apply across different services according to the degree of influence they are able to exert in shaping community views. With the emergence of new technologies and new media, and the expansion of the broadcasting regulatory regime, new and unforeseen challenges and competing objectives have arisen. This has led to a practical shift away from the 'degree of influence' principle.

Traditional broadcasting services are highly regulated. The new content services legislation now places some restrictions on internet and mobile content. However notwithstanding these restrictions, the Internet is subject to much less regulation than traditional media. New business models are emerging for the delivery of services that are similar to television and radio over the Internet, mobile and other means. As these take on greater mass appeal and usage and become more influential, this sharpens the divergence in approach to these services compared with more traditional broadcasting services, and reveals the growing lack of consistency between their actual regulation and their degree of influence.

Expansion of the BSA

The BSA was introduced at a time where there was an established set of players and platforms for media. It sought to achieve its founding objectives by describing services according to their nature and not their technical means of delivery. Since its introduction, the BSA has been expanded with the insertion of regulatory regimes for digital television conversion, Internet services, pay television expenditure on new Australian and New Zealand drama, anti-hoarding, digital datacasting services, international broadcasting services and non-broadcast media content services.

The consequence of these ad hoc amendments has been a significant shift in the original assumptions underlying the BSA, namely that regulation would be technologically neutral and proportionate to the degree of influence of each service. The Communications Law Centre takes the view that despite its central place in the rhetoric under the BSA, 'degree of influence' is not, and should not be, central to the mechanisms of broadcasting regulation,[1] as it is uncertain and the different levels of regulation reflect a number of factors, only some of which are relevant to 'degree of influence'. The current BSA "does not contain one system of regulation. It contains several widely divergent regulatory schemes."[2] These divergent regulatory regimes for broadcasting, datacasting and online services appear to be based on diverging regulatory policies.

Overview

There are varying levels of regulation under the BSA.

Commercial broadcasting

Commercial television broadcasting services were deemed the most 'influential' category of broadcasting services in influencing community views, presumably because of the type of content they provide, and their ubiquity. It has been suggested this assumption was flawed in the first place and is becoming more outdated as time goes by.[3]

Commercial television services are required to comply with wide ranging requirements in relation to licensing and licence fees, licence conditions, content codes, Australian content, classification, advertising, and stringent ownership and control rules. Radio is perceived to be less likely than television to influence the community. It is subject to licence conditions and codes of practice which are less prescriptive than TV.

Subscription television

Subscription television requirements are less extensive, and include content rules relating to censorship, local content and anti-siphoning. It has been argued some of these are unnecessarily onerous in consideration of its 'degree of influence', including in particular the anti-siphoning rules.[4]

Open narrowcasting

By contrast, 'open narrowcasting services' are barely regulated at all, subject to a class licensing scheme and minimum licence conditions, with no restrictions on Australian content or ownership and control. This reflects the perception that they are less influential than other broadcasting services on community views, given their specialist scope.

Streaming

The advent of 'streaming video and audio' services has meant that content previously identifiable as television or radio programs can now be streamed over the Internet and accessed via a range of delivery platforms. This raised uncertainties as to whether these services would be considered 'broadcasting services' [5] and thus regulated by the BSA. This led to concerns from the Internet industry[6] that if they were regulated, given the moratorium on the issue of new licences this would effectively give existing licence holders exclusive rights and drive other providers offshore,[7] with adverse effects on the emerging Internet industry in Australia.

In September 2000 the Minister for Communications, Technology and the Arts formally determined that:

> *a service that makes available television programs or radio programs using the internet, other than a service that delivers television or radio programs using the broadcasting services bands*

did not fall within the definition of 'broadcasting service' in subsection 6(1) of the BSA.[8]

Therefore streaming audio and video services are not broadcasting services if they are delivered using the Internet or via phone networks to mobile phones. This provides opportunities for content providers to provide television or radio programs over the Internet, without a licence and free from BSA regulations. However, some new limited regulation is now provided under the content services legislation.

Content Services

The new Schedule 7 of the BSA, effective 1 January 2008 (and related codes), places restrictions on all non-broadcast media content services delivered via carriage services, which covers the internet, mobile phones and other convergent devices. This prohibits X18+ and RC content, and requires providers to restrict access to MA15+ and R18+ content from children under 15 and 18 respectively. Content providers may be required to remove content on complaint. This extends the internet regulatory framework established under Schedule 5 (and closes some of its loopholes) and repeals those parts that applied to content services.

Effectively this provides protection to minors from unsuitable content. Otherwise however, these services are not subject to BSA requirements relating to licensing, Australian content or ownership rules.

Regulatory Asymmetries

Under the current regulatory regime, content which looks or sounds the same from the perspective of the audience may be regulated in different ways depending on how that content is delivered.[9] Providers will be prejudiced or favoured depending on their chosen delivery method and whether they exploit the loopholes, and this will significantly impact the way services are delivered.

Television and radio programs will be subject to BSA restrictions when transmitted using conventional broadcast technology, but are subject to a more limited regulatory regime when delivered via the Internet or telephone networks.

A movie on demand service where users are able to start, stop, rewind and forward the video would not constitute a broadcasting service because it makes programs available on demand on a point-to-point basis. If movies are delivered via a carriage service they would be subject to Schedule 7 but not other broadcasting rules. Pay television channels such as Foxtel Box Office delivered continuously on a point to multi-point basis to subscribers are broadcasting services and subject to the BSA.

Computer game consoles that allow access to the Internet, personal digital assistants such as Blackberries that download and display video, and mobile phones that receive services that sound like commercial radio and television, are subject to Schedule 7 but not subject to other broadcasting rules, as long as they do not use the BSB.[10]

The above examples illustrate the mismatch between the amendments to the BSA and the BSA's 'foundation principles'. These distinctions do not seem appropriate in a converging communications environment. This results in competing businesses, and even services within the same business, being subjected to separate regulatory regimes, which can inefficiently distort investment and consumption choices.[11] Unintended consequences of regulation are likely to be particularly pronounced in markets characterised by uncertainty.[12] In such circumstances, clear and appropriate regulatory objectives are imperative.

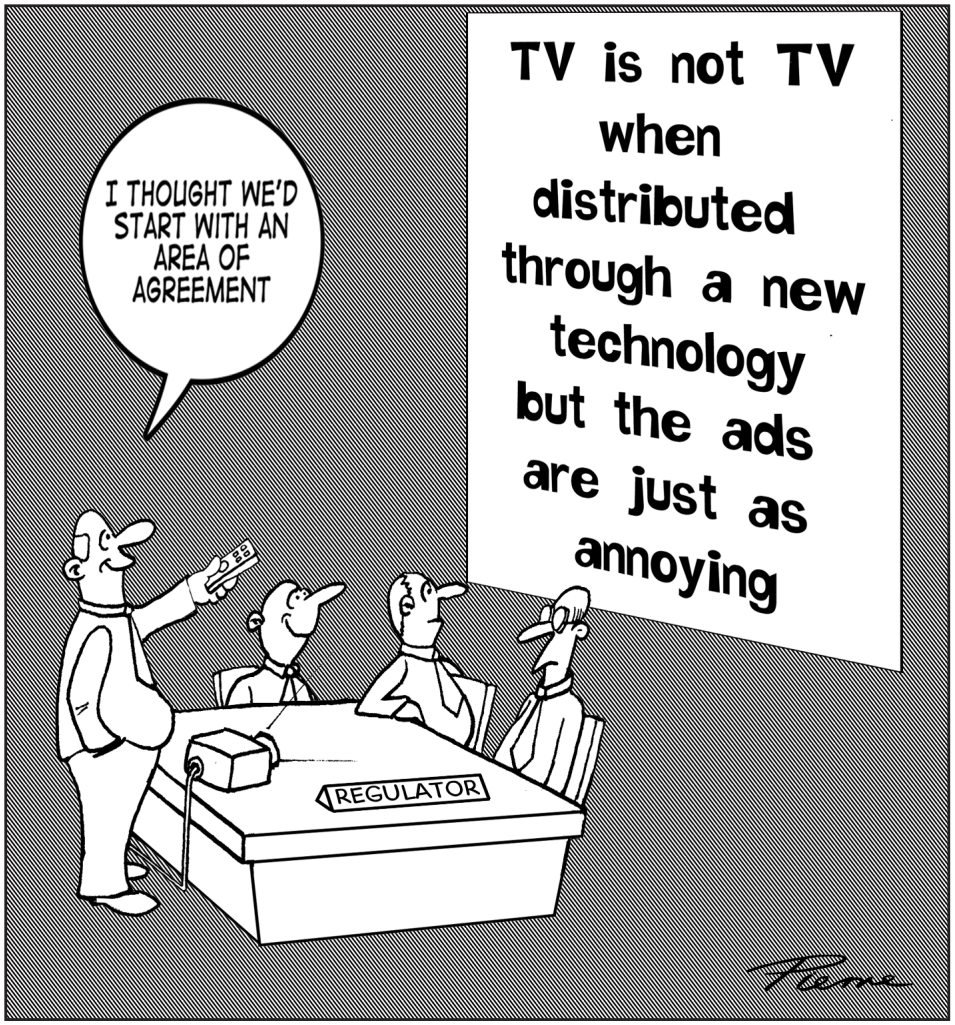
The content services legislation is a significant step in regulating content across a range of different platforms in a consistent manner. This neutral approach to the means of delivery should be embraced on a broader basis. However it is fairly limited in nature and there still remains a stark divide in how these services are treated compared with other more traditional media. This may need to be revisited as these services become more widespread and competitive.

As new media services gain more of a foothold in the Australian media landscape the regulatory incongruence will be highlighted. In particular the regulatory constraints on traditional media such as commercial television, compared to those imposed on competing new media alternatives, will become even more out of step with their degree of influence over the community. This raises questions whether the existing regulatory approach is sustainable.

Shifts in Influence

Internet

Recent years have seen the dramatic rise in the pervasiveness and influence of the Internet as a medium. The proliferation of independent blogs, news sites, social networking and other online sources of content, has led to increasing competition with traditional media. For a growing base of users, these are equally valid sources of news, political commentary, information and entertainment. They are able to shape and indicate public opinion and have a significant influence on popular culture and politics.



For example, sites like MySpace and YouTube have dedicated political areas, where politicians have profiles, launch policies and interact with users. Following the US where the Internet is a powerful campaigning strategy, the Australian 2007 Federal election was dubbed the 'e-election'.[13] The Internet has growing influence on the views and experiences of the "internet generation." This raises the prospect of the role of traditional broadcasting in public discourse becoming increasingly marginalised.

Almost seventy five per cent of Australians are current Internet users[14] and online advertising has been growing exponentially in recent years. In 2008 advertisers spent over $1.5 billion advertising online, up 27% on 2007.[15] New media alternatives are placing increased pressure on television and other media, with commercial TV revenue growth dropping and the profitability of commercial networks falling in recent years.[16]

Regulation of broadcasting is recognition that the media, particularly broadcasting, is an important and essential source of information for the community.[17] Internet services are not subject to BSA requirements as to fair and accurate news reporting, or adequate coverage of matters of local significance.

The Government has taken a general policy stance of not over regulating the Internet, to advance competitive Internet technologies and business within Australia. It has also responded to pressures suggesting that over regulation of new media would drive business offshore. However these overriding policy objectives have little to with those of traditional broadcasting regulation. The ever increasing influence of the Internet only further exposes the divergence of regulatory policy from the 'degree of influence' principle. As time goes on, underestimating the influence of the Internet may result in an imbalance amongst different media platforms. To enable regulation to develop in a forward thinking, coherent way, it is necessary to re-evaluate and clarify these principles to apply across all communications.

Convergence and technology

Ongoing media convergence is eroding the boundaries between telecommunications, broadcasting and the Internet, and telecommunications networks are increasingly seeking to compete in the delivery of broadcast services.[18]

Increasing network speeds have allowed for the delivery of audiovisual content over the Internet. Without ownership or control restrictions, new and existing players are free to take advantage of opportunities in new media.

Most Australian media mainstays have their own new media organisations, and firms from outside the media such as Telstra are also moving into media-related activities.[19] A host of players are already providing TV programs, games, movies and content via the Web and mobile phones.[20] BigPond has its own online TV channel.[21] MySpace TV and Youtube have recently launched original drama series produced directly for the Internet, with distribution deals for other platforms.[22] Original "snack dramas" are now available in Australia via mobile phone networks. These shows can incorporate social networking and interactivity. Traditional broadcasters are lagging in responding to these trends, although they are increasing their focus on delivery of program downloads and cross-platform content. In the UK, ITV Local, which streams full local Internet TV services, has proved so successful it is being rolled out nationally.[23] Its founders provide over 100 Internet TV channels around the world.

The rise of Internet TV and related services will shift power from broadcasters to other organisations that can provide comparable services over new platforms. These services do not have to comply with BSA requirements including ownership, fair and accurate news reporting, diversity, and community standards. Rules requiring minimum Australian content, that help promote the role of broadcasting in reflecting Australia's cultural identity, are not applicable to online or mobile services, providing little incentive for them to be culturally appropriate, or Australian. While the digital age promises increased diversity, empire building is still a natural tendency with many promising Internet businesses being snapped up by larger players.

As the platforms available for 'convergent' services become more pervasive and the boundaries between the broadcasting and telecommunications industries become increasingly blurred, the separation of the various regulatory regimes is likely to be more difficult to sustain.

What is Driving Regulation?

It can no longer be said that the driving principle of regulation is degree of influence. While the 'degree of influence' test still applies to some extent in shaping traditional broadcasting regulation, it appears to have lost its central importance in the context of non-broadcasting services which have been brought within the scope of the BSA. Other more pressing concerns have arisen with new technologies and services, including the need to preserve investment, and develop and protect local media businesses.

The decision to exclude Internet radio and video services from 'broadcasting services' was based not on their degree of influence, but on unrelated considerations such as the promotion of investment and development in Australia for these technologies and services.[24] It clearly showed the Government's willingness to allow Internet radio and video services to develop with a much lower level of regulation for the time being.

The main driving factor of the original online legislative regime (Schedule 5) was the protection of children, rather than the 'degree of influence'. In the Productivity Commission Broadcasting Inquiry, it was suggested the test was particularly undermined by these online amendments,

> *whose interventions are informed less by any understanding of the degree of influence of online media than by the kind of naively apocalyptic vision of media power and influence which so often accompanies the introduction of new technologies.*[25]

Australian content services legislation has recognised the growing need for consistent regulation across new media platforms and provides some restrictions. Here the policy objective was again the protection of children, but heavily influenced by the need to harmonise regulation of content, accommodate technological change and to encourage the development of technologies.[26] It is apparent that the degree of influence principle has taken a back seat in driving new areas of regulation. The central regulatory principles underpinning the BSA need to be restated and simplified.[27]

New media has the capacity to rapidly become highly influential, and remains difficult to regulate. There are strong arguments why some of the traditional BSA rules may still not be appropriate to new media services, given their more flexible, fragmented and developing nature. Allowing this area to develop will enable innovative content models to prosper. However, these artificial regulatory distinctions are strained and regulation is out of step with its founding objectives.

Conclusion

The general policy rationale of the BSA for regulating some broadcasting services more than others is the intention that different levels of regulatory control be applied according to their 'degree of influence'. However as new technologies have emerged and new legislative regimes have been introduced into the BSA, there has been a shift away from this principle and other objectives have taken precedence. The regulation of new technologies has been increasingly motivated by other factors including the protection of investment, the interests of incumbent broadcasters, and the advancement of technologies. As the Internet grows in dominance, and convergent technologies facilitate the provision of more influential content, this sharpens the divide in regulation and highlights the diminished relevance of the 'degree of influence' principle. Arguably the 'degree of influence' principle is outmoded and more suited to the bygone era where you were able to 'silo' media into neat, distinct groups and treat them differently. This needs to be revisited to ensure that clear consistent regulatory objectives are established across all communications, which recognise the competing pressures in a converging environment.

Heidi Bruce is a Senior Associate in the Sydney office of Anisimoff Legal, advertising and marketing law firm

(Endnotes)

1 Submission to Productivity Commission Review of the Broadcasting Services Act 1992, June 1999.

2 Flint, D, Australian Broadcasting Authority Chairman, 2000.

3 Australian Broadcasting Authority, *Broadcasting Regulation in Australia 1992-1997 – a Five Year Report Card on the Broadcasting Services Act 1992* (15 October 1997).

4 M McCutcheon, *Is Pay TV Meeting its Promise?* Thesis, Murdoch University (2006) at 389.

5 Second Reading Speech, *Broadcasting Services Amendment (Digital Television and Datacasting) Bill 2000*.

6 See for example: Internet Industry Association; J Czechowicz, 'First Compressions' *Management Today* (2000).

7 Davies, 'Industry fears of ban on streaming soothed' *Sydney Morning Herald* (20 July 2000).

8 Commonwealth Government Gazette 2000.

9 C Lidgerwood *Reactive, Not Proactive: Recent Trends in Australian Broadcasting Regulation* (2002).

10 C Lidgerwood above n 9 at 25.

11 M Landrigan, 'Competition Policy and Convergence – is there a need for industry specific regulation?' (2000) 19(3) *CLB* 1.

12 Id at 4.

13 A Moses, 'Pollies embrace Google for the "e-election"' *Sydney Morning Herald* (14 September 2007).

14 CCI Digital Futures Report *The Internet in Australia* (July 2008).

15 PricewaterhouseCoopers *IAB Online Advertising Expenditure Report* (August 2008).

16 Australian Communications and Media Authority *Commercial Television Industry Financial Trends 1978-79 to 2005-06.*

17 L Hitchens, 'Commercial Broadcasting – Preserving the Public Interest' *Federal Law Review* (2004).

18 See M Landrigan above n 11.

19 Productivity Commission *Broadcasting Inquiry Report* (2000) at 113.

20 See: for example Bigpond, see also Grover, R 'Murdoch's Tech Offensive' *Business Week* (5 June 2006).

21 www.bigpondtv.com.

22 Rueters 'MySpace TV unveils first original web drama' *Sydney Morning Herald* (22 October 2007); Baxter, E 'The Rise of snack drama' *Sydney Morning Herald* (27 March 2008).

23 S Finlayson 'Tuning into Internet TV' *Broadcast Engineering News* (December 2006).

24 Department of Communications Information Technology and the Arts *Report to Parliament: Review of audio and video streaming over the internet* available at: www.dcita.gov.au.

25 See: Communications Law Centre 2000.

26 Department of Communications Information Technology and the Arts *Review of the Regulation of Content Delivered over Convergent Devices* April 2006.

27 C Lidgerwood above n 9 at 27. In 2000, a UK White Paper recommended a high level set of principles for regulation of content across all electronic communications, to be administered by one merged regulator. See: UK Departments of Trade and Industry and of Culture, Media and Sport *A New Future for Communications* (December 2000).

You Can't Always Get What you Warrant

Kieran Mahony and Tara Walker consider the conflict between protection of information under Australian law and disclosure compelled by overseas laws

Introduction

Individuals and companies involved in the supply of telecommunications in Australia are subject to a general requirement to protect the confidentiality of subscriber information and the content of communications under the regime for protection of communications contained in Part 13 of the *Telecommunications Act 1997* (Cth) (the ***Telecoms Act***). The prohibition on disclosure is subject to various exceptions, which are set out in Division 3 of Part 13.

Carriers and Carriage Service Providers (***CSPs***) also have obligations under the *Telecommunications (Interception and Access) Act 1979* (Cth) (***Interception Act***) in respect of access to and use of 'stored communications'.

This article considers a hypothetical dilemma in which an Australian Internet Service Provider (***ISP***), with operations located in the United States, is served with a warrant to produce information by an American law enforcement agency, for example the Federal Bureau of Investigation (***FBI***), requiring disclosure of confidential information in circumstances that are not covered by the exceptions and therefore could involve breach of Australian law (***FBI Scenario***). A company in such a situation would potentially be forced to choose between breaching Australian law or facing contempt charges or other consequences in the jurisdiction in which the warrant is issued.

Companies may be able to avoid or minimise the risk of encountering this problem. In particular, terms and conditions of standard customer agreements can be drafted to try and bring confidential information within the ambit of knowledge or consent disclosure exceptions in the legislation.[1] The extent to which this approach adequately shields companies from liability is considered below.

The issue also justifies attention from the communications regulator, the Australian Communications and Media Authority (***ACMA***). The industry would benefit from guidance as to how to deal with this situation (or avoid it in the first place).

How and why the problem arises

Accessing confidential information in Australia - policy context

The extent to which law enforcement agencies should be allowed access to confidential information in the interests of law enforcement and national security has been the subject of much debate in contemporary legal and political discourse. Heightened security concerns are often relied upon by governments to justify changes in the balance between the privacy rights of individuals and the investigative and enforcement capabilities of the state.[2]

The many security and privacy implications stemming from the increasing flow of information across borders have also been widely considered at an international level.[3] Australian law clearly recognises that there are circumstances in which it will be desirable to compromise the confidentiality of private information in the interests of security, including where that information is in the possession of non-Australian telecommunications carriers operating in Australia. The tension between security and privacy concerns is manifested in the dichotomy between the general prohibition against disclosure of confidential information in Division 2 and the exceptions in Division 3 of Part 13 of the Telecoms Act. The content of Part 13 of the Telecoms Act, along with relevant provisions in the Interception Act in relation to 'stored communications', will be considered in greater detail below.

Despite the apparent potential for this conflict of obligations to arise, there is little guidance for companies as to how to deal with the problem. This is presumably a reflection of the fact that the problem simply was not anticipated when the legislation was drafted.[4]

Intersection of laws

Although not considered in the telecommunications legislation, the conflict issue has been contemplated in other related areas. Notably in the Australian context, the *Privacy Act 1988 (Cth)* (***Privacy Act***) states in section 13D that:

> *An act or practice of an organisation done or engaged in outside Australia and an external Territory is not an interference with the privacy of an individual if the act or practice is required by an applicable law of a foreign country*.[5]

Frustratingly for telecommunications operators, this provision does not protect them, as Part 13 of the Telecoms Act operates concurrently with the Privacy Act. The recently released Australian Law Reform Commission report on Australian Privacy Law and Practice (***ALRC Privacy Report***) notes several submissions calling for a more consistent approach to privacy regulation in the field of telecommunications.[6] Suggestions to the ALRC included that Division 3 be removed from Part 13 and to allow the Privacy Act to solely regulate the exceptions field, or that Part 13 be completely moved into the Privacy Act. Nevertheless, the ALRC Privacy Report concludes that both Acts should continue to separately regulate privacy in the telecommunications industry, on the grounds that it is appropriate for the use and disclosure of the particular type of information covered by Part 13 (i.e. subscriber information and the contents of communications) to be subject to more stringent rules than those in the Privacy Act.[7]

Protection of communications under the Telecoms Act

The Telecoms Act does not refer specifically to ISPs, but applies to them because they fall within the category of carriage service providers.[8] CSPs supply communications services to the public using carrier infrastructure. Part 13 aims to protect privacy in communications by restricting CSPs (including ISPs), carriers, telecommunications contractors and their respective employees ('eligible persons')[9] from using or disclosing information relating to:

a) the contents of communications that have been, or are being, carried by carriers or CSPs (delivered or not); and

b) carriage services supplied by carriers and CSPs; and

c) the affairs or personal particulars of other persons.[10]

Electronic communications such as emails and instant messages may contain information falling within at least two of these categories: they contain both content of communications (the body of the email or message), and personal particulars of both subscribers and the recipients of their communications, such as identity, source, path and destination details. Emails are stored and forwarded 'at successive points along their journey to a nominated address', with the final point in the journey being the recipient's ISP computer or mail server, where they reside until accessed by the recipient.[11]

With regards to Australian ISPs with servers located and operated outside Australia by third party contractors, the extra-territorial application of the Telecoms Act[12] means that these servers fall within the ambit of Part 13.

Eligible persons must not use or disclose any information or document that relates to any of the three categories mentioned above and that came to their knowledge or into their possession in the course of carrying on their businesses.[13] Subject to the exceptions (discussed below), use or disclosure in contraven-

tion of this section is an offence punishable on conviction by imprisonment for a term not exceeding 2 years. [14]

Exceptions

The prohibitions against disclosure in Part 13 of the Telecoms Act are subject to a number of exceptions as set out in Division 3 of that Part. Whilst these are extensive,[15] they do not appear to apply in a situation such as the FBI Scenario, leaving Australian ISPs exposed to the risk of a conflict between complying with their obligations under Part 13 and relevant laws overseas.

The exceptions include situations where the use or disclosure is: made by an employee in the performance of duties for the carrier as employer;[16] required or authorised under an *Australian* warrant or *Australian* law;[17] made to ACMA or the Australian Competition and Consumer Commission (***ACCC***) to assist in carrying out their functions and powers,[18] made with the knowledge or consent of the person concerned;[19] made with the implicit consent of the sender and recipient of the communication;[20] for prescribed business needs of other carriers or service providers;[21] or permitted under the regulations.[22]

Disclosure authorised by or under law

As mentioned, it appears that these exceptions only apply where the authorisation or requirement is under Australian law.[23] Paragraph 280(1)(a) permits disclosure or use in connection with the operation of an enforcement agency, where the disclosure or use is required or authorised under a warrant. 'Enforcement agency' has the same definition as in the Interception Act and appears to be limited to Australian enforcement agencies.[24] The second limb of the exception (in paragraph 280(1)(b)) relates to disclosure or use required or authorised by or under law, and this is presumably limited to Australian law.

Under the Privacy Act, by contrast, if an organisation:

> *reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles*

then it may transfer personal information to someone who is in a foreign country.[25] Further, an act or practice of an organisation done or engaged in outside Australia and an external Territory is not an interference with the privacy of an individual if the act or practice is required by an applicable law of a foreign country.[26]

As identified by the ALRC, it is doubtful whether sections 280 or 297 of the Telecoms Act would allow a telecommunications service provider (such as an ISP) to rely on the more expansive exceptions of the Privacy Act *in addition to* those exceptions contained in the Telecoms Act. [27] Even if they did, not all ISPs would be caught by the Privacy Act due to the small business exception;[28] and in any event, compliance with Part 13 is a carrier licence condition, so would arguably need to be complied with by carriers irrespective of the operation of the Privacy Act.[29]

The ALRC has also recommended an additional exception under Part 13 for circumstances where a person 'has reason to suspect that unlawful activity has been, is being, or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities.'[30] If such an exception were introduced, eligible persons finding themselves in a position analogous to the FBI Scenario could potentially seek to utilise it to justify 'reporting its concerns to relevant persons or authorities' such as the FBI. Query, however, whether this exception is intended for persons who actively initiate their own investigations, as opposed to those who are merely responding to and assisting with the investigation of another body. Query also whether 'relevant persons or authorities' could be read as extending to a foreign law enforcement agency.

Consent exceptions

An alternative means by which an Australian ISP could deal with a situation such as the FBI Scenario is to use its standard terms of service and/or privacy policy to try and bring itself within one of the consent options under Division 3.[31] Section 289 states that disclosure or use by a person of information or a document will not be prohibited if:

> *a) the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person; and*
>
> *b) the other person:*
>
> *(i) is reasonably likely to have been aware or made aware that information or a document of that kind is usually disclosed, or used, as the case requires, in the circumstances concerned; or*
>
> *(ii) has consented to the disclosure, or use, as the case requires, in the circumstances concerned.*

Section 290 contains an 'implicit consent' exception. It provides that disclosure or use is not prohibited if:

> *(d) the information or document related to the contents or substance of a communication made by another person; and*
>
> *(e) having regard to all of the relevant circumstances, it might reasonably be expected that the sender **and** the recipient of the communication would have consented to that disclosure or use, had they been aware of the disclosure or use.*

The contrasting language used in these two sections reflects the distinction between the two main types of information protected under this Part. The 'affairs or personal particulars' referred to in section 289 covers subscriber information (for example the names, addresses and other details of customers). The 'contents or substance of a communication' referred to in section 290 pertains to the actual information contained in a communication (for example the contents of emails or SMS messages).

Different thresholds apply to each of these exceptions. For the disclosure of subscriber information (section 289), the carrier need only show that the customer is 'reasonably likely to have been aware or made aware that information or a document of that kind is usually disclosed' in the circumstances. In the FBI Scenario, this requirement might be satisfied if the ISP's terms of service or standard customer agreement included a provision to the effect that confidential information will be handed over to a law enforcement agency – domestic or otherwise – in circumstances where it is validly sought under applicable legislation from the ISP or a related company.

In their respective privacy policies applicable to the provision of email services, ISPs such as Microsoft[32], Google[33] and Yahoo!7,[34] all include terms whereby subscribers must consent to the transfer, storage and processing of personal information on servers located outside the country in which they reside. These policies also contain terms reserving the ISP's rights to access personal information in limited circumstances, including where a reasonable belief is held that disclosure is necessary to comply with applicable laws and process. Read together, these terms arguably provide a basis upon which the ISPs can argue that they have obtained the implicit consent of the subscriber, at least in respect of accessing subscriber information.

For the disclosure of the content of a communication, the threshold is higher. To be covered by the exception in s 290, the carrier must show that:

> *it might reasonably be expected that both the sender **and** the recipient of the communication would have consented to the disclosure or use, if they had been aware of the disclosure or use*.

The extent to which this exception applies may again depend on the standard terms and conditions issued by the individual ISP, however the difficulty is establishing that the recipient of the communication (who is not a party to the agreement) of the communication implicitly agreed to the disclosure.

Protection of communications under the Interception Act

Carriers and CSPs also have obligations under the Interception Act in respect of access to and use of 'stored communications'.[35] The definition of 'stored communication' has a number of elements. The communication must:

- not be passing over a telecommunications system (it is only stored once it has ceased passing over a system - communications in the process of passing may not be intercepted without a warrant, or unless some other exception applies);
- be held on equipment operated by, and in the possession of, a carrier; and
- cannot be accessed on that equipment, by a person who is not a party to the communication, without the assistance of an employee of the carrier.[36]

'Carrier' in this context is defined to include a CSP. While this would include an Australian ISP, it may not extend to include a foreign company operating a server located overseas on behalf of the ISP. If an overseas warrant were issued seeking content held on a server or equipment owned by the Australian ISP, but operated in the relevant overseas jurisdiction by a third party contractor, it is possible that content would not actually constitute 'stored communications' because it would not be 'held on equipment operated by and in the possession of' the Australian ISP.

Carriers and CSPs who are in possession of stored communications within the meaning of the Interception Act are obliged under subsection 108(1) of the Interception Act not to:

a) access a stored communication; or

b) authorise, suffer or permit another person to access a stored communication; or

c) do any act or thing that will enable the person or another person to access a stored communication,

without the knowledge of the intended recipient of the stored communication and the person who sent the stored communication.

A person is taken to have 'knowledge' if they are given written notice of an intention to access. This appears to entail written notice of an intention to do a *specific* act or thing, rather than a general notice as to the possibility of access occurring at some stage. Accordingly, the 'knowledge' requirement may not be satisfied simply by an ISP including a general access provision in its customer terms and conditions. However, a subscriber to an email or messaging service is presumably the intended recipient of messages in the 'inbox', and the sender of messages in the 'sent mail' box. In this light, a specific written notice to the relevant subscriber could possibly satisfy the knowledge requirement.

Breach of section 108 of the Interception Act is punishable on conviction by imprisonment for 2 years or 120 penalty units ($13,200) or both.

Exceptions

Subsection 108(2) of the Interception Act contains a number of exceptions to the obligations set out in subsection 108(1), including exceptions relating to warrants issued under the Interception Act, the activities of

Australian law enforcement agencies, and where access is reasonably necessary to perform a person's duties (relating to installation, connection or maintenance of equipment etc). None of these exceptions appear to apply in circumstances where a warrant is issued in another jurisdiction for access to the content of a communication classified as a stored communication for the purposes of the Interception Act.

How the FBI Scenario may be dealt with in practice

The ISP may be assisted by the relevant mutual assistance agreements between Australia and the United States as a means of legitimately exchanging the necessary information.[37] A formal request for the information in question by the Australian authorities, pursuant to an arrangement with their US counterparts, would appear to bring the disclosure under the law enforcement exception in section 280 of the Telecoms Act. It appears that analogous situations are commonly dealt with in this way.

Assuming any breach was identified by ACMA and referred to the Commonwealth Department of Public Prosecutions (***CDPP***), the circumstances may not support the taking of further action by the CDPP. As outlined above, there are 'common sense' alternatives available to resolve the problem, and the CDPP's guidelines indicate that relatively trivial matters, or minor breaches of a 'technical' nature, will not meet the requisite public interest threshold for prosecution.

Conclusion

The FBI Scenario raises a technical legal point along with some interesting policy issues. The potential for conflicting legal obligations to arise for Australian ISPs operating abroad is presumably an unintended result of the overlap of the legislative regimes of different jurisdictions (and an inherent deficiency within that the regimes as the problem was not foreseen), combined with the rapid globalisation of telecommunications and associated increase in trans-border information exchanges. Anecdotal information suggests that ACMA and the Attorney-General's Department (which administers the Interception Act) are aware of the issues and perhaps should consider providing general guidance on the issue. As outlined in this paper, such measures include the use of appropriately drafted terms and conditions to bring potential disclosures of confidential information within the ambit of the legislative exceptions, or alternatively seeking the involvement of the Australian authorities under the relevant bilateral mutual assistance arrangements.

Kieran Mahony and Tara Walker are Lawyers at Clayton Utz in Sydney

(Endnotes)

1 Refer to sections 289-290 of the Telecoms Act. Matching secondary disclosure exceptions (by persons authorised to receive such information under Division 3) are contained in Division 4, sections 296-303A.

2 In Australia, this shift is arguably reflected in various pieces of legislation, for instance the *Anti-Terrorism Act 2005 (Cth)*.

3 See, e.g., the Asia-Pacific Economic Cooperation (***APEC***) Privacy Framework, the Organisation for Economic Co-operation and Development (***OECD***) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and the European Parliament and the Council of the European Union (***EU***) Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

4 The opposite scenario could presumably also occur - where a non-Australian operator with activities in Australia could find itself in breach of its own domestic regulations - if it complies with disclosure requirements of Australian law enforcement agencies.

5 See also subsection 6A(4), which states that the National Privacy Principles are not breached by an act or practice required by an applicable law of a foreign country.

6 ALRC Privacy Report, Chapter 71 'Telecommunications Act', paragraphs 71.44 - 71.46.

7 ALRC Privacy Report, Chapter 71 'Telecommunications Act', Id, paragraphs 71.49-71.50.

8 Australian Communications and Media Authority, *Internet Service Providers and Law Enforcement and National Security Fact Sheet*, accessed on 22 July 2007 at http://www.acma.gov.au/WEB/STANDARD?pc=PC_100072

9 Telecoms Act, s 271.

10 Telecoms Act, s 276(1)(a).

11 T Starey, 'Getting the message: law enforcement agencies' access to stored communications' (2005) 10(1) *MALR* 25.

12 Telecoms Act, s 9.

13 Telecoms Act, sub-s 276(2).

14 Telecoms Act, sub-s 276(3).

15 It has recently been argued that the exceptions 'permit uses and disclosures of personal information for a broader range of purposes than the National Privacy Principles' which 'can result in diminished protections for personal information in the telecommunications sector', Office of the Privacy Commissioner, 'Submission to ALRC Review of Privacy', Issues Paper 31 (February 2007), p 396. Available at http://www.privacy.gov.au/publications/alrc280207.html

16 Telecoms Act, s 279.

17 Telecoms Act, ss 280 and 297 (secondary disclosure).

18 Telecoms Act, s 284.

19 Telecoms Act, s 289.

20 Telecoms Act, s 290.

21 Telecoms Act, s 291.

22 Telecoms Act, s 292.

23 Similarly, s 313 of the Telecommunications Act (which provides that a carrier is not liable for damages for an act done or omitted in good faith to give reasonably necessary assistance to officers and authorities of the Commonwealth, States, or Territories) applies only in relation to Australian law.

24 Interception Act, section 5. Note that the definition lists a number of Australian enforcement agencies (a) - (m), but also includes '(n) any body whose functions include administering a law imposing a pecuniary penalty.' There is no suggestion however that this would extend to foreign law enforcement bodies.

25 National Privacy Principle 9.

26 Privacy Act, s 13D.

27 See ALRC Privacy Report, paragraphs 72.27 - 72.30. Note that the ALRC has recommended amending sections 280 and 297 to clarify that the exception does not authorise a use or disclosure that would be permitted by the Privacy Act if that use or disclosure would not otherwise be permitted under Part 13 of the Telecoms Act (ALRC Privacy Report, Recommendation 72-1). Interestingly, section 303B provides for the reverse: disclosure or use permitted under Part 13 is taken to be authorised for the purposes of the privacy legislation.

28 See ALRC Privacy Report, paragraphs 39.52 - 39.57, which identifies the telecommunications industry as a 'high-risk sector' due to the large number of ISPs who fall within the small business exception based on a turnover of less than $3 million per annum.

29 Telecoms Act, Schedule 1.

30 ALRC Privacy Report, Recommendation 72-2.

31 Telecoms Act, ss 289 and 290.

32 Microsoft Online Privacy Statement: http://privacy.microsoft.com/en-au/fullnotice.aspx

33 Google Privacy Policy: http://www.google.com/privacypolicy.html

34 Yahoo!7 Terms of Service: http://au.docs.yahoo.com/info/terms/ and Yahoo!7 Privacy Policy: http://info.yahoo.com/privacy/au/yahoo/

35 Interception Act, s 108.

36 Interception Act, s 5.

37 Refer to the CDPP website page on 'international work': http://www.cdpp.gov.au/Practice/International.aspx. The formal mutual assistance regime relies on a network of international relations, and the goodwill of countries to assist each other in the investigation and prosecution of criminal matters. It is governed by the Mutual Assistance in Criminal Matters Act 1987. The United States has a 'Treaty with Australia on Mutual Assistance in Criminal Matters'. The formal regime runs parallel with a less formal system of international cooperation between investigating agencies.

Australian Domain Name Policy

Rebecca Sadleir discusses the new auDA policy and the relaxation of rules on transferring .au domain name licences

auDA, the Australian Domain Name Administrator, has introduced a policy which removes most of the restrictions which previously applied to the transfer of *.au* domain name licences from one person to another. The procedure for transferring *.au* domain names has also been simplified. The Transfers (Change of Registrant) Policy (2008-08) (the ***Policy***) came into effect on 1 June 2008.

auDA is the government-endorsed policy authority and industry self-regulatory body for the *.au* domain space. It is responsible for developing and implementing policies in relation to the *.au* domain space, as well as accrediting and licensing domain name registrars and facilitating the .au Dispute Resolution Policy. auDA also represents Australia at ICANN – the Internet Corporation for Assigned Names and Numbers, the organisation which co-ordinates the naming systems for the internet – and other international forums.

Background

There are no proprietary rights in a *.au* domain name, and it is not strictly possible to 'sell' a domain name. This is because a registrant does not 'own' the name itself; instead, it holds a licence to use the domain name for a specified period, subject to certain terms and conditions. However, it is possible to transfer a domain name licence in certain circumstances, and it is this which is addressed by the new auDA Policy.

Historically, both the registration and transfer of domain name licences in the *.au* space have been subject to strict controls. Although restrictions have gradually been eased over the last few years, the rules were (and indeed still are) significantly more stringent than those for domain names in many other countries and, for example, in the *.com* space.

Before the implementation of the Policy, transfer of a *.au* domain name licence was permitted only in specific, limited, circumstances. For example, it was not possible to transfer a domain name from one entity to another for purely commercial reasons, unless in the context of a wider business sale. In addition, the transfer process was relatively cumbersome and, amongst other things, required the transferee to make a statutory declaration confirming that the circumstances of the transfer complied with the relevant rules.

The new policy

On 1 June, after several months of public consultation, auDA introduced the Policy. As a result, subject to certain conditions which are discussed below, the holder of a domain name can now offer its domain name licence for sale, and may transfer it to another eligible entity for any reason.

The auDA 2007 Names Policy Panel, which undertook two rounds of public consultation and produced an issues paper and recommendations prior to implementation of the new policy, identified a number of policy objectives for the *.au* domain:

- to maintain the Australian identity of the *.au* domain space;
- to enhance the usability of the *.au* domain space;
- to preserve the integrity of the *.au* domain space; and
- to facilitate economic benefits flowing from the *.au* domain space.

The Policy attempts to strike a balance between these various objectives, with the emphasis on enhancing usability and facilitating economic benefits.

Relaxation of transfer rules

Under the Policy, subject to one prohibition which is discussed below, the holder of a domain name registration may:

- offer its domain name licence for transfer (or 'sale') to another eligible entity, by any means; and
- transfer its domain name licence to another eligible entity, for any reason.

The result of this is to permit a secondary market in *.au* domain names, such as has existed for many years in the *.com* space. However, it is intended that the restrictions described below will operate to prevent that secondary market from becoming a 'free for all', and ensure that the system is in line with the policy objectives outlined above.

Prohibition on transfer within six months of registration

It is a fundamental rule of *.au* domain name registration that a person may not register a domain name for the sole purpose of resale or transfer to another entity. This basic rule is not altered by the new Policy.

In order to support this principle, and in an attempt to minimise cybersquatting, scams and misuse of domain name registrations, the Policy prohibits a registrant from transferring its domain name licence within the first six months after registration. This prohibition applies to newly registered domain names only, and not to renewed or transferred domain names.

A registrant may apply to auDA for authorisation to transfer its domain name licence within the first six months after registration. Any authorisation will be at auDA's discretion. The policy provides that circumstances in which auDA may authorise a transfer include:

- where a competent arbitrator, tribunal, court or legislative body orders the registrant to transfer its domain name licence to the proposed new registrant, eg in the case of a proceeding under the *.au* Dispute Resolution Policy; or
- where the registrant and the proposed new registrant belong to the same corporate group, such as where a parent company transfers its domain name licence to a subsidiary.

Eligibility and allocation rules

As noted above, two of the considerations which auDA took into account in formulating the Policy were the desire to maintain the Australian identity of the *.au* domain space, such that *.au* registrants have an association or nexus with Australia; and the need to preserve its integrity by minimising cybersquatting and other misuse of *.au* domain name registrations, and reduce conflicts and disputes.

Those considerations are addressed by the relevant eligibility criteria, which must be met by any person wishing to hold a domain name licence, including a transferee under the Policy. These are not altered by the policy, and are set out in auDA's Domain Name Eligibility and Allocation Policy Rules for Open 2LDs (2008-05).

To be eligible to hold a *.com.au* domain name, the registrant must be 'Australian'. This means that it must be either an Australian registered company; trading under a registered business name in Australia; an Australian partnership or sole trader; a foreign company licensed to trade in Australia; the owner of, or applicant for, an Australian trade mark or application; an association incorporated in Australia; or an Australian commercial statutory body.

In addition, domain names in the *.com.au* domain must be either an exact match, abbreviation or acronym of the registrant's name or trade mark, or otherwise must be 'closely and substantially connected' with the registrant. There will be a 'close and substantial connection' if, for example, the domain name is the name of a product that the registrant manufactures or sells; a service it provides; or an event that it organises or sponsors.

In a further development in the direction of relaxing the rules governing *.au* domains, the Domain Monetisation Policy (2008-10) issued on 30 June 2008, clarifies that 'domain monetisation' falls within the category of 'a service which the registrant provides'. Domain monetisation is registering a domain name in order to earn money from a 'monetised website', that is, a website or 'landing page' which has been created for the purpose of earning revenue from advertising, including monetised domain parking pages.

There are other, similar (but generally more restrictive) eligibility criteria for other *.au* second-level domains, such as *.org.au*, *.asn.au* and *.net.au*.

Procedure and effect of transfer

The Policy sets out standard wording that a domain name licence transfer application must now contain. This includes short declarations from both the transferor and transferee as to their authorisation to submit the form, to transfer the domain name and, in the case of the transferee, that it is eligible to hold the domain name under the eligibility rules. This replaces the previous, more burdensome procedure, which involved providing documentary evidence of the transfer, as well as a statutory declaration by the new registrant detailing the circumstances of the transfer.

As before, a transfer will result in a new two-year domain name licence being issued to the proposed new registrant. The previous registrant is not entitled to be reimbursed for the unused portion of its domain name licence. Parties to a transfer may be asked to disclose the sale method and price, on a voluntary and confidential basis, so that auDA can collect aggregated statistical data.

The auDA policy review panel recommended that the Policy be reviewed after two years. It remains to be seen whether these changes will result in a significant increase in domain name trading; it should at least make life easier for those wishing to sell their domain name for legitimate reasons.

Rebecca Sadleir is a Senior Associate in the Intellectual Property practice group at Allens Arthur Robinson in Sydney

Communications & Media Law Association Incorporated

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

Issues of interest to CAMLA members include:

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

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

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

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

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:

Page Henty

C/- AUSTAR Entertainment Pty Ltd
Wilcox Mofflin Building
46-52 Mountain Street
ULTIMO NSW 2007
Tel: +61 2 9295 0153
Fax: +61 2 9295 0163
Email: phenty@austar.com.au

Matt Vitins

C/- Allens Arthur Robinson
Deutsche Bank Place
Corner Hunter & Phillip Streets
SYDNEY NSW 2000
Tel: +612 9230 4000
Fax: +612 9230 5333
email: matt.vitins@aar.com.au

Lesley Hitchens

C/- Faculty of Law,
University of Technology Sydney
PO Box 123
BROADWAY NSW 2007
Tel: +61 2 9514 3694
Fax: +61 2 9514 3400
Email: lesley.hitchens@uts.edu.au

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, Box 545, Glebe NSW 2037
Tel/Fax: +61 2 9660 1645

Name:.....

Address: .....

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

Principal areas of interest: .....

.....

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

☐ I Ordinary membership $130.00 (includes GST)

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

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

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

Signature: .....