

# Copyright Conundrum – Liability of ISPs for Online Copyright Infringement

Gaye L. Middleton

Lawyer

KAZ Technology Services Pty Ltd  
Sydney, New South Wales

gaye.middleton@kaz-group.com

## Abstract

As digital rights holders become increasingly proactive in asserting their rights against infringers, Internet service providers (“ISPs”) are more frequently becoming embroiled in online copyright infringement disputes. ISPs have, in turn, become increasingly concerned about their potential exposure to liability for acts of copyright infringement committed by their subscribers using the ISPs’ facilities and services, and about balancing their privacy obligations to subscribers with compliance with requests for disclosure of subscriber details by digital rights holders who allege that those subscribers have committed acts of copyright infringement. This paper examines the potential liability of ISPs under Australian law for acts of online copyright infringement by their subscribers, both before and after the implementation of the U.S.-Australia Free Trade Agreement. It also considers the obligations of ISPs to disclose subscriber details to digital rights holders who allege that those subscribers have infringed their digital rights. Finally, this paper briefly discusses ways in which ISPs can minimise their liability through their contractual relationship with subscribers.

## 1 Introduction

The Internet has opened a wide range of opportunities for sharing, not only information, but also art, music, literature and other works, in a global arena. While these opportunities provide undeniable benefits to Internet users, they have caused great concern amongst owners of copyright in works and audio-visual items. These concerns arise because the nature of the Internet makes it more difficult for copyright owners to maintain control over the use and distribution of works and audio-visual items and to enforce their rights in the online environment than in the “bricks and mortar” world. Reasons for these difficulties include the ability for multiple copies of online materials to be created rapidly in a large number of locations, the global availability of online materials, and the ability for Internet users to make themselves virtually anonymous. Given these difficulties, it is not surprising that copyright owners have turned to

ISPs to assist them with enforcing their rights, and as alternative defendants in copyright infringement actions involving online infringement. This is because, unlike their subscribers, ISPs are readily identifiable, and can control whether or not an individual can use their facilities to access the Internet. In the United States, the practice of copyright owners relying on ISPs to assist them to enforce their digital rights has received legislative backing in the form of section 512 of the U.S. Copyright Act (17 U.S.C.). This section limits the remedies available against ISPs for copyright infringement if their conduct falls within the scope of the four “safe harbours” introduced in 1998 by the U.S. Digital Millennium Copyright Act (“DMCA”). Under the DMCA provisions, ISPs must, among other things, comply with a notice and take down procedure in respect of infringing materials, and disclose details of infringing subscribers to copyright owners pursuant to a subpoena requesting those details.

While this trend of turning to ISPs to assist in the enforcement of digital rights is beneficial to copyright owners, it has alarmed ISPs and their subscribers alike. ISPs believe that, because they cannot control and are usually not aware of the online conduct of their subscribers, they should not be held liable for acts of their subscribers which infringe copyright merely because the ISPs make available the facilities used for such infringing acts. Further, both ISPs and their subscribers are concerned about the privacy implications if copyright owners are able to obtain details of allegedly infringing subscribers from ISPs without any judicial intervention.

In the United States, some ISPs and their subscribers strongly oppose the notice and take down provisions in section 512 of the U.S. Copyright Act, as they believe that some copyright owners are using these provisions to arbitrarily suppress content on the Internet, without conducting proper due diligence or providing reasonable evidence of infringement (e.g. see Birchall, 2003 and Manjoo, 2003). ISPs in the U.S. are also concerned about the costs associated with complying with subpoenas obtained by copyright owners under section 512(h) of the U.S. Copyright Act, which require ISPs to disclose to copyright owners such information as is required to identify an alleged copyright infringer. Concerns over the privacy implications and costs burden associated with complying with these subpoenas have led some U.S. ISPs to challenge subpoenas issued to them under section 512(h) of the U.S. Copyright Act (e.g. see *Recording Industry Association of America, Inc. v Verizon Internet Services, Inc.* 351 F.3d 1229; *Pacific Bell Internet*

*Services v Recording Industry Association of America Inc.*, N.D.Cal. 3560 JL, filed 30 June 2003).

These concerns have recently come to the forefront in Australia, following the passing into law of the *U.S. Free Trade Agreement Implementation Act 2004* (Cth) ("FTA Act") on 16 August 2004. This Act implements the Australia-U.S. Free Trade Agreement ("FTA"), including Article 17.11.29 regarding limitations on liability of ISPs and other service providers. Through amendments to the *Copyright Act 1968* (Cth) ("Copyright Act"), the FTA Act introduces into Australian copyright law provisions similar to those in section 512 of the U.S. Copyright Act. These amendments have once again fuelled the debate regarding the rights of copyright owners versus the rights of ISPs and Internet users.

This paper considers the liability of ISPs for acts of copyright infringement by their subscribers both before and after implementation of the FTA, including the obligations of ISPs to disclose the details of alleged infringers to copyright owners, and to what extent ISPs can limit their risks through contractually managing their relationship with their subscribers.

## 2 Copyright - Pre-FTA Position

### 2.1 The Digital Agenda Act

In a bid to address the challenges posed to Australian copyright law by emerging digital technologies, the Australian government passed the *Copyright Amendment (Digital Agenda) Act 2000* (Cth) ("Digital Agenda Act"), amending the Copyright Act. According to the Australian government's commentary on an exposure draft of the Digital Agenda Act, the central aim of the reforms introduced by that Act was to ensure that copyright law continued to promote creative endeavour while allowing reasonable access to copyright material through the Internet and new communications technology.

### 2.2 Right of Communication to the Public

One of the key reforms introduced by the Digital Agenda Act was to introduce a new right of communication to the public ("communication right"), being a technology neutral right to replace the former technology specific broadcasting and cable diffusion rights. The new communication right includes the digital rights of copyright owners. "Communicate" is defined in section 10 of the Copyright Act as making available online or electronically transmitting a copyright work or other subject matter. Under section 10(1) of the Copyright Act, "to the public" means to the public within and outside Australia. There is no further elucidation of the meaning of the phrase "to the public" in the Copyright Act. However, in the High Court of Australia's decision in *Telstra Corporation Limited v Australasian Performing Right Association Limited* ("APRA") (1997) 38 IPR 294 at 302 ("Telstra Decision"), "to the public" was held for the purposes of copyright law to mean to the copyright owner's public, regardless of the size or physical setting of the audience.

### 2.3 ISP liability

In the Telstra Decision, the majority of the High Court of Australia found that Telstra had infringed the cable diffusion rights of various music copyright owners by providing a music on-hold service to users of fixed telephone services without the copyright owners' permission, even though Telstra did not always provide or select the music played on-hold. Subsequently, APRA filed proceedings for copyright infringement against Ozemail, an Australian ISP, seeking damages for infringement of the cable diffusion right in musical works owned by APRA by transmission of those works over Ozemail's network without APRA's permission ("Ozemail Proceedings"). This case was settled before trial, but commentators believe that if it had proceeded to trial, APRA would have been successful (e.g. see Mercurio, 2002).

In response to the Telstra Decision and the Ozemail Proceedings, the Digital Agenda Act introduced a variety of reforms designed to clarify the liability of communications carriers and ISPs for acts of copyright infringement facilitated by the use of their facilities or services. These reforms are as follows:

1. Section 22(6) of the Copyright Act, dealing with the right of communication to the public, is a deeming provision that was introduced to make it clear that the person who determines the content of a communication is the person who is deemed to have made that communication, not the communications carrier or ISP over whose facilities or services that communication is made. This provision overcomes the finding of the High Court in the Telstra Decision that Telstra, as the person operating the fixed line telephone service over which music on-hold was transmitted, was the person making the infringing transmissions of the musical works in question (Hakim, 1999 and Middleton, 1999).
2. Sections 36 and 101 of the Copyright Act were introduced to codify the law regarding authorisation infringement. Under section 13(2) of the Copyright Act, one of the exclusive rights of a copyright owner is to authorise others to exercise any of the rights of the copyright owner. Pursuant to the decision of the High Court of Australia in *University of New South Wales v Moorhouse and Angus & Robertson (Publishers) Pty Ltd* (1975) 133 CLR 1 ("Moorhouse"), a person authorises a copyright infringement if that person sanctions, approves or countenances the infringement. Sections 36 and 101 of the Copyright Act are based on the factors found to indicate the sanction, approval or countenance of copyright infringement by the High Court in Moorhouse. These sections provide that when determining whether or not a person has authorised copyright infringement, the court must consider (a) whether that person has the power to prevent an infringing act; (b) the relationship between that person and the

person who conducted the infringing acts; and (c) whether that person took reasonable steps to prevent or avoid the infringing act, including whether that person complied with any relevant industry codes of practice. Currently, there are no relevant industry codes of practice in Australia (Phillips Fox, 2004).

3. Sections 39B and 112E of the Copyright Act were intended to make it clear that carriers and carriage service providers such as ISPs will not be taken to have authorised copyright infringement merely because the facilities that they provide for making a communication are used by a person to infringe the copyright of another. A similar provision exempts carriers and carriage service providers from authorisation liability for infringements of moral rights under section 195AVB of the Copyright Act. Among those persons who made submissions to the review of the Digital Agenda Act commissioned by the Australian Attorney-General's Department, there was consensus that these provisions have not achieved their intended purpose (Phillips Fox, 2004). If the matter of *Universal Music Australia Pty Ltd v E-Talk & Anor* (Federal Court proceeding no. N1551 of 2003) proceeds to trial, it will be the first time that the meaning of sections 39B and 112E will be considered by the Australian courts (Phillips Fox, 2004 and Ceola, 2003). In these proceedings, an ISP is being sued by a major record company for allowing allegedly infringing MP3 music files to be downloaded from a website hosted by that ISP.

When the Digital Agenda Act was introduced, the Australian federal government deliberately left the liability of ISPs for online copyright infringement to be determined by the law applicable to authorisation liability. This position has been criticised as an unproductive way of determining the liability of ISPs for online copyright infringement, as the more that an ISP tries to prevent copyright infringement, and hence is perceived to have power to prevent an infringing act, then the greater the risk that the ISP will become liable for authorisation infringement (Fitzgerald, 2000).

## 2.4 Exclusion for Temporary Reproductions

Prior to the Digital Agenda Act, there was concern among Internet users in Australia that, because browsing the Internet involves the making of temporary copies of materials which are the subject of copyright in the memory of the user's computer, then Internet users could be liable for infringement of the copyright owner's exclusive right to reproduce those materials. To address this concern, the Digital Agenda Act introduced sections 43A and 111A into the Copyright Act, which provide that a person does not infringe copyright in online materials by making a temporary reproduction or adaptation of those materials as part of the technical process of making or receiving a communication, provided that the making of the communication does not itself infringe copyright.

A common practice among ISPs is "proxy" or "forward" caching, which involves an ISP deliberately making a copy of popular websites on its proxy server so as to make access to these websites quicker and less costly (Baird, 2001, IPCR, 2000 and Garlick and Nicholls, 1999). The general view among legal commentators is that it is unlikely that proxy caching (as opposed to passive or automatic caching) is covered by the temporary reproductions exceptions in sections 43A and 111A of the Copyright Act, as reproductions of copyright materials made in the course of proxy caching are arguably not temporary, and are not made as part of the technical process of making or receiving a communication (Baird, 2001, IPCR, 2000 and Garlick and Nicholls, 1999).

In the Ergas Report (IPCR, 2000), the Australian Intellectual Property and Copyright Review Committee ("Committee") recommended that, to the extent that sections 43A and 111A of the Copyright Act do not cover proxy caching, then they should be amended, as the Committee considered that proxy caching promotes greater network efficiencies and reduced costs. For these reasons, the Committee was of the view that proxy caching provides important benefits to Internet users and to the development of e-commerce in Australia.

In the report concerning the review of the Digital Agenda Act commissioned by the Australian Attorney-General's Department ("Digital Agenda Review") (Phillips Fox, 2004), it states that no submissions in support of proxy caching (referred to as "active caching") demonstrated that any efficiency gains by ISPs were passed on to consumers. Accordingly, there is no recommendation in the Digital Agenda Review that sections 43A and 111A be amended so as to permit proxy caching (Phillips Fox, 2004).

## 3 Copyright – Post-FTA Position

### 3.1 FTA and Copyright

Article 17.11.29 of Chapter 17 of the FTA deals with limitations on liability for "service providers", including providers or operators of facilities for online services or network access such as ISPs. Schedule 9 Part 11 of the FTA Act implements this Article by inserting new Division 2AA of Part V into the Copyright Act. These provisions will come into force on the later of 1 January 2005 or the date on which the U.S. and Australian governments exchange notes approving of each other's legislative implementation of the FTA.

Unlike the fair dealing provisions in Division 3 of Part III of the Copyright Act, these new provisions do not create exclusions from copyright infringement. Rather, these provisions limit the remedies that are available against ISPs and other carriage service providers ("CSPs") for copyright infringements that relate to carrying out certain categories of online activities if those CSPs comply with certain specified conditions.

### 3.2 "Safe Harbours" and Limitation of Remedies

The categories of online activities in sections 116AC to 116AF of the Copyright Act to which the limitation on remedies under section 116AG apply are similar to the four “safe harbours” of the U.S. DMCA, and are as follows:

1. Providing facilities or services for transmitting, routing or providing connections for copyright material, or intermediate and transient storage of copyright material in the course of those activities (“Category A activity”);
2. Caching copyright material through an automatic process, where the ISP has not manually selected the copyright material to be cached (“Category B activity”);
3. At the direction of a user, storing copyright material on a system or network controlled or operated by or for the ISP (“Category C activity”); and
4. Referring users to an online location using information location tools or technology (“Category D activity”).

If an ISP satisfies the conditions in section 116AH(1) of the Copyright Act that apply to the above categories of activities, and that ISP infringes copyright in carrying out any of those activities, then under section 116AG(3) of the Copyright Act, a court may only grant the following relief against that ISP for those infringing acts:

1. In respect of Category A activities, an order requiring the ISP to block access to online locations outside of Australia or to terminate the account of an infringing subscriber; and
2. In respect of Categories B, C or D activities, an order requiring the ISP to remove or block infringing materials and references to those materials, terminate the account of an infringing subscriber or another less burdensome but comparably effective non-monetary order.

When deciding what orders to make against an ISP in respect of copyright infringements arising from the relevant categories of activities, a court must have regard to the following factors under section 116AG(5):

1. The harm caused to the relevant copyright owner;
2. The burden that the order will place on the ISP;
3. The technical feasibility of compliance with the order; and
4. Whether another comparably effective order would be less burdensome.

Where section 116AG applies to an ISP, a court cannot grant monetary relief against that ISP, including damages, an account of profits or additional damages.

### 3.3 Conditions on Limitation of Remedies

To qualify for the limitation of remedies in section 116AG of the Copyright Act in respect of any of the four

categories of “safe harbour” activities, section 116AH(1) requires ISPs to:

1. adopt and implement a policy for terminating the accounts of repeat infringers; and
2. comply with the provisions of any relevant industry code for accommodating and not interfering with standard technical protection measures that protect and identify copyright material.

It is submitted that the better view is that a “repeat infringer” for the purposes of section 116AH of the Copyright Act is a person who has been found liable by a court for acts of online copyright infringement on two or more occasions, and is not simply a person against whom there has previously been unproven allegations of copyright infringement, whether in a “take down” notice by a copyright owner (see discussion below) or otherwise.

Currently, there are no relevant industry codes of conduct for the purposes of section 116AH (Phillips Fox, 2004).

In addition to these two general requirements, section 116AH(1) prescribes specific conditions that an ISP must comply with in order to qualify for the limitation of remedies. Where an alleged copyright infringement relates to a Category A activity, the relevant transmission of copyright material must have been initiated by a person other than the ISP (e.g. a subscriber), and the ISP must not substantively modify the copyright material transmitted, other than as part of a technical process.

The term “technical process” is not defined, but in this context, presumably means the process of providing a carriage service, which process modifies materials transmitted via that service without deliberate intervention by the ISP. The Explanatory Memorandum to the FTA Act cites “format shifting” necessary to provide access to copyright material via different technologies as an example of such a technical process.

Where the alleged copyright infringement arises in the course of a Category B activity, then to qualify for the limitation of remedies, an ISP must:

1. ensure that access to a significant part of any cached copyright material that is subject to certain conditions of access at the originating site is only available to users who have satisfied those conditions;
2. where there is a relevant industry code in force, comply with any provisions of that code dealing with updating cached copyright material and non-interference with technology used at the originating site to obtain information about the use of that material;
3. expeditiously remove or disable access to cached copyright material on receiving notice in the prescribed form that the material has been removed or blocked at the originating site; and

4. not substantively modify the copyright material transmitted, other than as part of a technical process.

If an alleged copyright infringement arises in the course of a Category C or D activity, then to qualify for the limitation of remedies, an ISP must:

1. not receive a financial benefit that is directly attributable to the infringing activity if the ISP has the right and ability to control that activity;
2. expeditiously remove or block access to (that is, "take down") copyright material residing on its system or network on receipt of notice in the prescribed form that a court has found that material infringes copyright; and
3. comply with the prescribed procedure for removing or blocking access to infringing material residing on its system or network.

For the purposes of condition (1), the FTA Act provides that a financial benefit is to be regarded as directly attributable to an infringing activity only if the ISP knew or ought reasonably to have known that a copyright infringement was involved. The elements of condition (1) are similar to the U.S. concept of vicarious liability, under which a person is vicariously liable for another person's infringing acts where that person has the right and ability to control the infringer's acts and receives a direct financial benefit from the infringing acts (*A & M Records Inc v Napster Inc* 239 F.3d 1004, 1022 (9<sup>th</sup> Cir. 2000)). In the decided U.S. Internet cases concerning vicarious liability for copyright infringement, there are cases which apply vicarious liability narrowly and other cases which apply it more broadly (Strachan, 2004). In those cases where vicarious liability is applied narrowly (e.g. see *Hendrickson v eBay Inc*, 165 F.Supp. 2d 1082 (C.D. Cal. 2001), *Ellison v Robertson* 189 F.Supp. 2d 1059 (C.D. Cal. 2002)), the courts have found that the right and ability to control infringing acts requires more than having the ability to do something to detect and prevent copyright infringement (e.g. the right to remove or block access to infringing material). By contrast, in those cases where vicarious liability has been applied broadly, the courts have held that where a service provider reserves the right to monitor or take down online material (e.g. in its terms of use), the service provider has the right and ability to control its infringing acts (e.g. see *Perfect 10 Inc v Cybernet Ventures* 213 F.Supp. 2d 1146 (C.D. 2002)). Strachan (2004) provides a detailed discussion of these differing approaches. It remains to be seen how Australian courts will interpret the "right and ability to control" test in respect of the safe harbour for Categories C and D activities under the FTA Act.

Condition (2) relates only to the notice and take down procedure where a court has found that the material in question infringes copyright. This condition does not fulfil the requirement under Article 17.11.29(b)(iv)(D) that the Categories C and D safe harbours be conditional on an ISP expeditiously taking down material on its system or network on obtaining actual knowledge of infringement or becoming aware of facts or circumstances from which infringement is merely

apparent rather than confirmed by a court, such as an effective notification under Article 17.11.29(b)(ix). Presumably, this requirement will be fulfilled by regulations dealing with the notice and take down procedure referred to in condition (3) (Varghese, 2004).

The notice and take down procedure applicable to condition (3) will include notice by copyright owners and counter-notice by the allegedly infringing subscriber, as referred to in Article 17.11.29(b)(ix) of the FTA. Under Article 17.11.29(b)(x) of the FTA, the legislation implementing the FTA must provide that an ISP who takes down material in good faith on the basis of a notice issued by a copyright owner will be exempt from liability for any resulting claims, provided that, in respect of material residing on the ISP's system or network, it takes reasonable steps to promptly notify the person making the material available that it has done so, and that if that person makes an effective counter-notification and is subject to jurisdiction in copyright infringement proceedings, it takes reasonable steps to restore the material online unless copyright infringement proceedings are commenced within a reasonable time by the copyright owner who issued the original take down notice.

The essential form of notice to be given to ISPs pursuant to conditions (2) and (3) has already been agreed in side letters regarding ISP liability exchanged between Australia and the U.S. on 18 May 2004. These side letters, which form part of the FTA, list the information that must be included in an effective notice by a copyright owner or counter-notice by an allegedly infringing subscriber to an ISP to have the relevant material taken down or reinstated, as the case may be. For example, a notice by a copyright owner requiring an ISP to take down infringing material must include:

1. the name address, telephone number and email address of the complainant;
2. information that is reasonably sufficient to enable the ISP to identify the works claimed to have been infringed, and to identify and locate the infringing material;
3. statements that the complainant has a good faith belief that the allegedly infringing use is not authorised by the copyright owner, its agent or law, that the information in the notice is accurate, and that the complainant is the owner of copyright in the relevant material or their agent; and
4. the signature of the person giving the notice.

The notice and take down requirements in Article 17.11.29 of the FTA are modelled on the notice and take down provisions in section 512 of the U.S. Copyright Act. Under the U.S. notice and take down procedure, ISPs are taking down material based solely on notice of claimed infringement from copyright owners so as to take advantage of the relevant safe harbour. This has allegedly led to abuses by some copyright owners, who issue notices requiring removal or blocking of online material without conducting proper due diligence to

determine whether or not such material does infringe their rights, or for ulterior motives (e.g. to have competitors' websites removed) (Varghese, 2004, Clarke, 2004, Birchall, 2003 and Manjoo, 2003). Given the delay between the issue of a take down notice and the restoration of material following a counter-notification and the elapse of a reasonable time without the copyright owner commencing copyright infringement proceedings, in time critical situations the issue of a take down notice could effectively settle the matter in favour of the copyright owner without any judicial intervention (Varghese, 2004).

One commentator (Clarke, 2004) has expressed the view that if ISPs in Australia are required to take down allegedly infringing materials solely on the basis of a notice claiming infringement from the copyright owner, then without additional consumer protections being inserted into the Copyright Act, the potentially adverse effects in Australia would be greater than in the U.S., because:

1. the fair use provisions in the U.S. Copyright Act in respect of copyright materials are more substantial than Australia's fair dealing provisions, giving U.S. rights users greater protection; and
2. the U.S. Constitution protects the right of freedom of speech, for which there is no Australian equivalent.

User rights associations have further commented that in Article 17.11.29 of the FTA, there is no balancing incentive for ISPs to restore material which has been taken down on receipt of counter-notification, even if copyright infringement proceedings are not commenced by the copyright owner within a reasonable time (Australian Digital Alliance, 2004 and Electronic Frontiers Australia, 2004).

As no Australian draft regulations which deal with the notice and take down procedure have been released to date, it is not yet possible to determine whether that procedure will contain sufficient protections to guard against the abuses of the notice and take down procedure that are allegedly occurring in the U.S..

Pursuant to section 116AH(2) of the Copyright Act, it is not necessary for an ISP to monitor its services or to otherwise seek indications of infringing activities except to the extent required by a standard technical measure referred to in an industry code to protect and identify copyright material. The inclusion of this provision in the FTA Act will provide relief to many ISPs, who do not have the technical means, finances or resources to effectively undertake such a task (Mercurio, 2002). It will also provide some comfort to subscribers, the majority of whom would not wish for their activities to be monitored.

Under section 116AI of the Copyright Act, the onus of proving non-compliance with the conditions necessary for an ISP to take advantage of the limitation of remedies in section 116AG is on the person alleging non-compliance.

## 4 Obligations to Disclose Infringer Details

### 4.1 Current Disclosure Requirements

Currently, there are no provisions in the Copyright Act which deal with the disclosure by ISPs to copyright owners of the details of alleged online copyright infringers. Instead, copyright owners who require this information must rely on the ordinary pre-trial discovery provisions in the Australian *Federal Court Rules* and their State and Territory superior court equivalents.

These discovery provisions were applied in the online context in *Sony Music Entertainment (Australia) Limited v University of Tasmania* [2003] FCA 532 (30 May 2003) and [2003] FCA 724 (18 July 2003). In this case, Sony and two other international music companies ("the applicants") sought orders for discovery and inspection under Order 15A, rules 3 and 6 of the *Federal Court Rules* against the Universities of Tasmania, Sydney and Melbourne ("the respondents"). The applicants alleged that the respondents' computer systems were being used to infringe the applicants' copyright in certain sound recordings through unauthorised file swapping. To ascertain the identities of the persons responsible for the allegedly infringing acts and for authorising those acts, the applicants sought an order for discovery of backup copies and tapes of information stored on the respondents' servers under O15A, rr3 and 6 of the *Federal Court Rules*.

Under O15A r3, where an applicant is unable, having made reasonable enquiries, to sufficiently describe a person for the purposes commencing Federal Court proceedings against that person, and it appears that another person has or is likely to have possession of documents that would tend to assist in describing the person concerned, then the court may make an order for the discovery of all documents which are or have been in a person's possession which relate to the description of the person concerned. A similar order for discovery may be made by a court under O15A r6 where (i) the applicant has cause to believe that it may have the right to obtain relief against an identified person; but (ii) despite making all reasonable enquiries, the applicant does not have sufficient information to decide whether to commence proceedings to obtain that relief; and (iii) the applicant has a reasonable cause to believe that the person in question has in its possession any document relating to the question of whether the applicant has the right to obtain relief and that inspection of the document in question would assist the applicant to decide whether or not to commence proceedings to obtain that relief.

The respondents opposed the orders for discovery sought by the applicants on the basis that the production of such a large number of documents was not within the terms of O15A r3, and would therefore lead to the discovery of documents other than those relating to the description of persons concerned in alleged acts of copyright infringement. However, the respondents were agreeable to more narrow discovery of particular types of documents being made. They also submitted that the applicants had sufficient information to decide whether or

not they had the right to relief against the respondents for authorising infringement of copyright under O15A r6 without the discovery sought by the applicants.

Tamberlin J of the Federal Court of Australia held that, in deciding whether or not to grant orders for discovery under O15A rr3 and 6, the court must have regard to the fact that at the preliminary discovery stage, no issues have been formulated against which the relevance of documents can be measured. As the guidelines in O15A rr3 and 6 are in wide terms, the Judge held that some degree of “fishing” may be appropriate.

In deciding whether or not to exercise its discretion to make orders for discovery under O15A rr3 and 6, Tamberlin J held that the following factors must also be considered:

1. The public policy interest in protecting the privacy of those using the facilities of the person against whom the orders are sought;
2. The public interest in having full and proper disclosure by way of preliminary discovery to ensure that an informed decision can be made as to whether or not to commence proceedings, and against whom those proceedings should be brought; and
3. The interests of third parties regarding non-disclosure of privileged or sensitive matters which in no way concern the contemplated proceedings between the parties, but about whom information is contained in the material in respect of which discovery is sought.

The Judge held that the first of these considerations could be alleviated by express undertakings as to privacy, and by the established principles of discovery which prevent the misuse or abuse of information given on discovery or its use for purposes other than in the proceedings in which discovery was ordered.

Having regard to the above considerations, Tamberlin J held that the discovery sought by the applicants was too broad, as it would lead to the discovery of documents with no relevance to the proceedings, and could raise significant issues of legal privilege, confidentiality and privacy as well as relevance. However, the Judge found that the orders sought by the respondents were too narrow, and would be likely to lead to insufficient discovery.

Tamberlin J ordered that, provided that a strict undertaking as to non-disclosure and confidentiality was given by the applicants, then access to the requested records could be given to the applicants’ expert to search, then a copy of the information extracted by the searches from those records should be given to the respondents. Next, the Judge stated that the respondents should have an opportunity to make any claims for privilege or confidentiality, followed by the issue of an affidavit of discovery relating to all information produced by the expert’s searches that they concede is discoverable. Finally, the discoverable documents may be inspected by the

applicants. Following further submissions by the applicants and the respondents as to the form of this discovery process, orders were made by Tamberlin J to give effect to that process.

## 4.2 FTA Disclosure Requirements

Article 17.11.29(b)(xi) of the FTA requires Australia and the U.S. to provide for an administrative or judicial procedure which enables copyright owners who have given “effective notification” of claimed infringement to expeditiously obtain from ISPs and other service providers information in their possession that identifies alleged infringers. As with the notice and take down procedure, this procedure is not enacted in the FTA Act, and presumably will be dealt with in the subsequent regulations to accompany the FTA Act.

In submissions made to the Senate Select Committee on the U.S.-Australia Free Trade Agreement, ISPs, other service providers and privacy and consumer groups expressed the view that ISPs and other service providers should not be required to disclose subscriber information to copyright owners unless there is a court order made to that effect (Internet Industry Association, 2004, Electronic Frontiers Australia, 2004 and Australian Digital Alliance, 2004). In other words, these groups advocate that the regulations under the FTA Act provide for a judicial process rather than an administrative process. The main concerns expressed by these groups with respect to the disclosure of subscriber details by ISPs to copyright owners related to privacy issues, and the compliance burden that any such procedure would place on ISPs and other service providers (e.g. see Mitchell and Mackenzie, 2004). The prevailing view of service provider groups is that the existing procedure under O15A of the *Federal Court Rules* is sufficient, and that no changes are required to the existing law. In turn, they believe that this approach is the best way to safeguard the privacy rights of their subscribers.

### 4.2.1 U.S. subpoena procedure

The U.S. procedure which implements Article 17.11.29(b)(xi) of the FTA is section 512(h) of the U.S. Copyright Act. Under this provision, copyright owners may obtain details of an alleged infringer from ISPs by requesting a clerk of a United States district court to issue a subpoena to an ISP for identification of an alleged infringer. To obtain such a subpoena, a copyright owner must issue and provide a copy of a take down notice under the U.S. Copyright Act, together with a sworn declaration to the effect that the purpose for seeking the subpoena is to obtain the identity of an alleged copyright infringer, and that such information will only be used for the purposes of protecting that person’s copyright. An ISP to whom such a subpoena is issued must expeditiously disclose to the copyright owner the information required by the subpoena.

There is no provision for judicial assessment of the merits of such a subpoena, and once a take down notice has been issued, obtaining a subpoena has been described as little more than a formality (Birchall, 2003).

When Verizon Internet Services (“Verizon”) refused to comply with a subpoena obtained by the Recording Industry Association of America (“RIAA”), on the basis that Verizon was merely a passive conduit for the allegedly infringing activities (the equivalent of a Category A activity under the FTA Act) and hence was not subject to the notice and take down procedure or the subpoena disclosure procedure under section 512 of the U.S. Copyright Act, RIAA sought and obtained at first instance a court order against Verizon to enforce that subpoena (*Recording Industry Association of America v Verizon Internet Services, Inc.*, unreported, District Court for the District of Columbia, Bates J, 21 January 2003). The Judge in that decision held that there was no reason why a take down notice could not be issued in respect of the first “safe harbour”, even though there was no provision under that safe harbour for a notice and take down procedure.

While the Verizon decision was overturned on appeal (*Recording Industry Association of America, Inc. v Verizon Internet Services, Inc.* 351 F.3d 1229), both it and the proceedings for declaratory relief commenced by Pacific Bell Internet Services (*Pacific Bell Internet Services v Recording Industry Association of America, Inc.*, N.D.Cal. 3560 JL, filed 30 July 2003) have highlighted the concerns of ISPs, other service providers and rights users regarding the potential for misuse of the section 512(h) subpoena procedure by copyright owners. These concerns include:

1. privacy concerns; and
2. the burden of compliance on service providers through being inundated with subpoenas under section 512(h) (Birchill, 2003).

Both ISPs and copyright users are concerned that, as with the notice and take down procedure, the subpoena procedure under the U.S. Copyright Act could be used for ulterior motives (e.g. by stalkers). The burden of compliance on service providers is demonstrated by the fact that, as at 28 July 2003, the RIAA had served almost 1,000 subpoenas under section 512(h) of the U.S. Copyright Act seeking information to identify alleged copyright infringers (Tobin, 2004).

#### **4.2.2 Interaction between Disclosure and Privacy Obligations**

Australian ISPs must comply with certain privacy obligations under the *Privacy Act* 1988 (Cth). Pursuant to section 16A(2) of the *Privacy Act* and National Privacy Principle (“NPP”) No. 2 under that Act, an ISP must not disclose personal information collected by it other than for the purposes for which it was collected unless that disclosure falls within one of the exceptions under that Act. “Personal information” is defined in section 6 of the *Privacy Act* to include any information about an individual whose identity is apparent, or can be reasonably ascertained, from that information. Accordingly, the types of information collected by an ISP from its subscribers in the course of entering into a contractual relationship with those subscribers to provide

them with Internet access would generally be personal information.

One of the exceptions to the general prohibition on the disclosure of personal information other than for the purpose for which it was collected is under NPP 2.1(g), which permits the disclosure of personal information to third parties when that disclosure is required by law. It is submitted that, once the requisite procedure has been enacted pursuant to the FTA Act, the requirement for ISPs to disclose to copyright owners information regarding the identity of subscribers who are alleged to have infringed copyright on receiving “effective notification” of that alleged infringement, will fall within the exception in NPP 2.1(g). Under those circumstances, ISPs will be permitted to disclose personal information regarding their subscribers to copyright owners who have given effective notification of claimed infringement without breaching their obligations under the *Privacy Act*.

Under Part 13 of the *Telecommunications Act* 1997 (Cth), ISPs, as carriage service providers, are obliged to protect the confidentiality of information that relates to the content of communications that are or have been carried by those ISPs and the affairs or personal particulars of another person (Gunning, 2000). Section 276 of the *Telecommunications Act* makes it a criminal offence for an ISP to breach its confidentiality obligations under Part 13 of that Act. However, the disclosure of such information is permitted in certain limited circumstances.

One of the circumstances in which an ISP may disclose information to third parties that is protected under Part 13 of the *Telecommunications Act* is where the disclosure of that information is required or authorised by law. Accordingly, where a copyright owner has given effective notification of claimed infringement under the procedure prescribed by the regulations to the FTA Act, then the disclosure by an ISP of subscriber details to that copyright owner will be regarded as required or authorised by law, and the ISP will not infringe its obligations of confidentiality under Part 13 of the *Telecommunications Act*.

If an ISP makes a disclosure of information that is protected under Part 13 of the *Telecommunications Act*, that ISP is obliged under that Act to make a record of the disclosure in the prescribed form, and to report annually to the Australian Communications Authority regarding such disclosures. The Privacy Commissioner is charged with monitoring compliance with these recording and reporting obligations by ISPs and other service providers who are subject to Part 13 of the *Telecommunications Act*.

On the basis of the above legislation, it is submitted that the disclosure by ISPs of subscriber details under a subpoena regime that is substantially similar to that contained in section 512(h) of the U.S. Copyright Act will not conflict with its statutory obligations of privacy and confidentiality, as such disclosures will fall within the exceptions to those statutory obligations. However, ISPs must be careful not to expose themselves to contractual liability for breach of non-disclosure obligations with respect to subscriber details in any



contract that they may have with their subscribers (Phillips Fox, 2004).

## 5 Contractual management of subscriber copyright issues

Generally, ISPs will enter into a formal contract with their subscribers for the provision of Internet access to those subscribers. ISPs can use this contract to manage their liability exposure for copyright infringement by specifically prohibiting subscribers from using the ISP's services or facilities to commit acts of copyright infringement, and by requiring subscribers to indemnify the ISP in respect of any loss or damage suffered or incurred by the ISP as a result of any breaches of that prohibition.

ISPs should ensure that they incorporate adequate privacy provisions into their subscriber contracts, which deal with issues such as the purpose for which personal information about subscribers will be collected and appropriate consents from subscribers regarding the purposes for which such information may be used.

It is also recommended that ISPs include a term in their subscriber contracts which permits them to terminate the subscriber accounts of persons who breach the terms of their subscriber contract, including those persons who are "repeat infringers" for the purposes of section 116AH of the Copyright Act.

## 6 Conclusion

One of the findings of the Digital Agenda Review is that the amendments to Australian copyright law introduced by the Digital Agenda Act have failed to clarify the liability of ISPs for authorising copyright infringement (Phillips Fox, 2004). In light of this uncertainty, the "safe harbours" to be introduced into the Copyright Act by the FTA Act will provide some protection for ISPs by limiting the remedies available for copyright infringement against ISPs who meet the conditions of those safe harbours. However, there are also concerns among ISPs and consumer groups regarding the amendments to Australian copyright law to be introduced by the FTA Act, based on U.S. experiences with similar provisions. These concerns are primarily with respect to potential abuses of the notice and take down procedure and the privacy and compliance issues associated with the as yet unknown procedure for disclosure of infringing subscriber details to copyright owners. It remains to be seen whether implementation of the Australian legislation will avoid the problems experienced in the U.S. following implementation of the DMCA, on which the FTA copyright provisions were modelled.

(Author's note: The opinions expressed in this paper are those of the author, and are not necessarily those of KAZ Technology Services Pty Ltd.)

## 7 References

AUSTRALIAN DIGITAL ALLIANCE (2004): Submission to the Select Committee – Australia-United States Free Trade Agreement.

<http://www.digital.org.au/downloads/Subsenateselect.doc> Accessed 24-Aug-2004.

BAIRD, J. (2001): *Copyright and the Internet*. 57. Pymont, LawBook Co.

BIRCHALL, S. (2003): Copyright Crack Down - The Implications for Australian Internet Service Providers under a Free Trade Agreement between Australia and the United States. *Computers & Law* 52:25-29.

CEOLA, N. (2003): ARIA Launches World First Action Against ISP. *Computers & Law* 54. <http://www.nswscl.org.au/journal/54/Ceola.html>. Accessed 24-Aug-2004.

CLARKE, R. (2004): The Economic and Cultural Impacts of the Free Trade Agreement Provisions relating to Copyright and Patent Law. <http://www.anu.edu.au/people/Roger.Clarke/II/FTA17.html>. Accessed 24-Aug-2004.

ELECTRONIC FRONTIERS AU.S. TRALIA (2004): Intellectual Property and the AU-U.S.A. Free Trade Agreement. <http://www.efa.org.au/Publish/ipfta-paper.html>. Accessed 24-Aug-2004.

FITZGERALD, B. (2000): Internet Service Provider Liability. In *Going Digital 2000: Legal Issues for E-Commerce, Software and the Internet*. FITZGERALD, A., FITZGERALD, B., CIFUENTES, C. AND COOK, P. (eds). St Leonards, Prospect Media.

GARLICK, M and NICHOLLS, R (1999): Proxy Caching – The New Fair Dealing? *Telemedia* 3(2):13.

GUNNING, P. (2000): Legal Aspects of Privacy and the Internet. In *Going Digital 2000: Legal Issues for E-Commerce, Software and the Internet*. FITZGERALD, A., FITZGERALD, B., CIFUENTES, C. AND COOK, P. (eds). St Leonards, Prospect Media.

HAKIM, S. (1999): Copyright and the Liability of ISPs. *Law Institute Journal* 73(9):62-65.

INTELLECTUAL PROPERTY AND COPYRIGHT REVIEW COMMITTEE ("IPCR") (2000): Report – Review of Intellectual Property Legislation under the Competition Principles Agreement ("Ergas Report"). <http://www.ipcr.gov.au/IPAustralia.pdf>. Accessed 22-Aug-2004.

INTERNET INDUSTRY ASSOCIATION (2004): Submission to the Senate Select Committee on the Australia-U.S. Free Trade Agreement. [http://www.aph.gov.au/Senate/committee/freetrade\\_ctte/submissions/sub525.pdf](http://www.aph.gov.au/Senate/committee/freetrade_ctte/submissions/sub525.pdf). Accessed 24-Aug-2004.

MANJOO, F. (2003): AOL's Jekyll and Hyde Act. *Salon Magazine* (Feb. 2003). [http://www.salon.com/tec/feautre/2003/02/10/aol\\_file\\_sharing](http://www.salon.com/tec/feautre/2003/02/10/aol_file_sharing). Accessed 24-Aug-2004.

MERCURIO, B. (2002): Internet Service Provider Liability for Copyright Infringement of Subscribers: A Comparison of the American and Australian Efforts to

Combat the Uncertainty. *Elaw Journal* 9(4).  
<http://www.murdoch.edu.au/elaw/issues/v9n4/mercurio94nf.html>. Accessed 6-Aug-2004.

MIDDLETON, G. (1999): Copyright Beyond the Digital Frontier - Australia's Proposed Digital Agenda Reforms. *Journal of Law and Information Science* 10(1):52-81.

MITCHELL, S. AND MACKENZIE, K. (2004): ISPs in the Dark over Copyright. *Australian IT*. 9-Mar-2004.

PHILLIPS FOX (2004): Digital Agenda Review - Report and Recommendations. Commonwealth Attorney-General's Department.  
<http://www.ag.gov.au/DigitalAgendaReview/reportrecommendations>. Accessed 3-May-2004.

STRACHAN, J. (2004): The Internet of Tomorrow: The New-Old Communications Tool of Control. *E.I.P.R.* 3:123-136.

TOBIN, J. (2004): Monkey Business. *Intellectual Property Forum* 57:30-45.

VARGHESE, J. (2004): Guide to Copyright and Patent Law Changes in the U.S. Free Trade Agreement Implementation Bill 2004.  
<http://www.aph.gov.au/library/pubs/CIB/2004-2005/05cibAbstracts.htm#05cib03.pdf>. Accessed 24-Aug-2004.