Bond Law Review

Volume 16 | Issue 1 Article 7

2004

Wipo Treaties, Free Trade Agreement and Implications for ISP Safe Harbour Provisions (The Role of ISP in Australian Copyright Law)

YiJun Tian

Wipo Treaties, Free Trade Agreement and Implications for ISP Safe Harbour Provisions (The Role of ISP in Australian Copyright Law)

Abstract
[extract] Over the past few years, most member countries have adapted their Copyright Laws to meet the requirements of the WIPO [World Intellectual Property Organization] Internet Treaties or regional trade agreements, and also set up corresponding 'ISP safe harbour' in their new legislation. This article will examine and compare the ISP safe harbour provisions in the legislation of different countries, especially focusing on the U.S. and Japan, and draw on their successful experiences. Then, it will examine the 'ISP safe harbour' in current Australian copyright law, especially the new requirements (in terms of ISP liability) under the Australia-United States Free Trade Agreement. Some recent cases in the U.S. and Australia will also be used to illustrate the potential problems of current ISP legislation and the possible solutions. Finally, this article will try to provide some specific suggestions for legislative reform in Australia (such as suggesting that Australia establish a 'Seven day Notice Takedown Regime' with its own features), and will argue that the legitive reform must be consistent with Australia's current economic, social and legal circumstances.

Keywords
copyright law, internet service providers, ISPs, WIPO Copyright Treaty, WIPO Performances and Phonograms Treaty, ISP safe harbour, United States, Japan, Australia, Australia-United States Free Trade Agreement

WIPO TREATIES, FREE TRADE AGREEMENT AND IMPLICATIONS FOR ISP SAFE HARBOUR PROVISIONS (THE ROLE OF ISP IN AUSTRALIAN COPYRIGHT LAW)

By YiJun TIAN[*]

Introduction

In order to apply the regulatory provisions of the Berne Convention to the new digital environment,[1] the World Intellectual Property Organization (WIPO) adopted two related treaties, the WIPO Copyright Treaty (WCT), and the WIPO Performances and Phonograms Treaty (WPPT) in Geneva in December, 1996. They are often referred to as the 'WIPO Internet Treaties'.[2]

With the growth of the Internet, Internet Service Providers (ISPs) are facing potential liability for the acts of subscribers using their services to access, post, or download information. The appropriate standard of liability for access providers has become an important issue for legislators in all countries throughout the world.[3] As to this issue, the WIPO treaties provide that copyright liability should not apply to a person or entity serving as a conduit, who 'provi[des]…physical facilities for enabling or making a communication'.[4] However, the treaties have not provided a specific standard of liability for ISPs and has left this question to the individual countries to decide.[5] Besides the WIPO treaties, some treaties at the regional level (such as bilateral free trade

---

* Doctor of Juridical Science (SJD) Research Student, Faculty of Law, University of New South Wales.

1 See Mihály Ficsor, (1996), 'Towards a Global Solution: The Digital Agenda of the Berne Protocol and the New Instrument', in *The Future of Copyright in a Digital Environment* edit by P. Bernt Hugenholtz, vol 111 at 37.

2 Ginsburg, J. C. (2003). 'Book Review: Achieving Balance in International Copyright Law - The WIPO Treaties 1996: The WIPO Copyright Treaty and The WIPO Performances and Phonograms Treaty: Commentary and Legal Analysis. Jörg Reinbothe and Silke von Lewinski, 2002. Pp 581' in 26 *Columbia Journal of Law & the Arts*, at 201.

3 Holmes, L. H. (2001). 'Note and Comment: Making waves in statutory safe harbours: Reevaluating Internet Service Providers' liability for third-party content and copyright infringement.' In 7 *Roger Williams University Law Review*, at 215.

4 See 'Concerning Article 8' in *Agreed Statements Concerning the WIPO Copyright Treaty*, WIPO Doc. No. CRNR/DC/96 (Dec. 20, 1996) [Online] http://www.wipo.int/documents/en/diplconf/distrib/96dc.htm ; also see Holmes, L. H. (2001). at 233.

5 Supra Note 3, Holmes, L. H. (2001). at 233.

agreement) now also include the requirements on limiting ISP liability.[6]

Over the past few years, most member countries have adapted their Copyright Laws to meet the requirements of the WIPO Internet Treaties or regional trade agreements, and also set up corresponding 'ISP safe harbour' in their new legislation. This article will examine and compare the ISP safe harbour provisions in the legislation of different countries, especially focusing on the U.S. and Japan[7], and draw on their successful experiences. Then, it will examine the 'ISP safe harbour' in current Australian copyright law, especially the new requirements (in terms of ISP liability) under the Australia-United States Free Trade Agreement (FTA).[8] Some recent cases in the U.S. and Australia will also be used to illustrate the potential problems of current ISP legislation and the possible solutions. Finally, this article will try to provide some specific suggestions for legislative reform in Australia (such as suggesting that Australia establish a 'Seven day Notice Takedown Regime' with its own features), and will argue that the legitive reform must be consistent with Australia's current economic, social and legal circumstances.

The US ISP Safe Harbour

This article will start with the U.S. digital copyright law. This section will focus on the U.S. ISP 'safe harbour' legislation. It will introduce the main purposes of the safe harbour legislation and the specific conditions for ISPs obtaining the safe harbour immunity. It will also give some comments on the U.S. current ISP legislation. Some recent decisions in the U.S. courts will be referred to.

Purpose of DMCA Safe Harbour

Following the WIPO Internet treaties, the U.S. Congress passed the Digital Millennium Copyright Act (DMCA) in 1998. The DMCA includes an ISP 'safe harbour' provision in its second chapter (Title II: Online Copyright Infringement Liability Limitation (OCILLA)[9]), in order to establish a proper standard of liability for ISPs. In enacting the OCILLA, the US Congress mainly intended to achieve two purposes: one is for limiting the liability of ISPs for

6 Such as the Free Trade Agreement between the United States and Australia

7 According to the requirements of Australia-United States Free Trade Agreement (FTA), Australia shall import the ISP regime of the United States' DMCA to its legislation. So this article will particularly examine the United States' ISP provisions and potential problems in those provisions.

8 On 8 February 2004, Trade Minister Mark Vaile concluded an agreed text for the Australia-United States Free Trade Agreement with his US counterpart, Trade Representative Bob Zoellick.

9 See 'Title II - Online Copyright Infringement Liability Limitation' of the DMCA. It is also referred to as the Online Copyright Infringement Liability Limitation Act (OCILLA) by one commentator. See Holmes, L. H. (2001) at 233.

copyright infringement; the other is for protecting intellectual property from unauthorized online distribution.[10]

Definition of 'Service Provider' & Scope of Protections

The OCILLA has established specific parameters for both defining and limiting the liability of ISPs for their subscribers' online copyright infringement acts.[11] And it provides ISPs a large, sweeping immunity from copyright liability including monetary,[12] injunctive[13] and equitable relief.[14] However, this statutory exemption from liability is only available to 'qualified Internet services'[15] that fit the definition of 'service provider' within the statute.[16]

Different Definitions given by DMCA and Courts

As to the definition of 'service provider', section 512 (k) (1) of the DMCA provides:

> (A) As used in subsection (a), the term 'service provider' means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.
> (B) As used in this section, other than subsection (a), the term 'service provider' means a provider of online services or network access, or the operator of facilities therefore, and includes an entity described in subparagraph (A).

According to this provision, although the definition of a service provider for the purposes of the safe harbour for providing transitory communications services (in s512(a)) is somewhat narrower, the definition of a service provider

10 Band, J. and M. Schruers (2002). 'Symposium Copyright Law as Communications Policy: Convergence of Paradigms and Cultures - Safe Harbours against the Liability Hurricane: The Communications Decency Act and the Digtial Millennium Copyright Act.', in 20 *Cardozo Arts and Entertainment Law Journal* 295, at 303.

11 Holmes, L. H. (2001) at 234.

12 S 512(k)(1)(B) of the DMCA.

13 S 512 (a)-(d) of the DMCA

14 Folawn, C. (2003). "Comments: Neighborhood Watch: The Negation of Rights Caused by the Notice Requirement in Copyright Enforcement under the Digital Millennium Copyright Act" in *26 Seattle University Law Review* 979, at 991.

15 See s 512(k)(1)(A)-(B) of the DMCA.

16 See s 512(k)(1)(B) of the DMCA. ("the term 'service provider' means a provider of online services or network access, or the operator of facilities therefor"). See also, Fessenden, G. (2002). 'Peer-to-Peer Technology: Analysis of Contributory Infringement and Fair Use' in 42 *IDEA: The Journal of Law and Technology* 391, at 397.

providing other services (listed in s512(b)-(d))[17] is very broad. As Band and Schruers stated, the definition (broad term) would seem to 'encompass virtually every Internet or intranet provider or intermediary, including portal sites, search engines, universities, and intranet providers'.[18] However, the U.S. courts have not applied the statutory definition of ISP broadly.[19] In the *Napster case*, Napster provided MP3 transmission services through Peep-to-Peer technology. Napster's Peer-to-Peer software enables its end users freely to transmit/exchange the MP3 files to each other via 'Internet'. The court held that the 'Internet' cannot be considered 'a system or network controlled or operated by or for the service provider',[20] and 'Napster does not transmit, route, or provide connections (for allegedly infringing music files) through its system'.[21] Finally it concluded the ISP (Napster) did not qualify for the s512(a) safe harbour.[22] As a result of this case, it seems that most 'indirectly network services', which are operated / conducted only via Internet,[23] will be excluded from the ISP safe harbour of the DMCA.

Qualified Internet Services

As to qualified Internet services, OCILLA (Safe Harbour provisions of the DMCA) limits ISP liability for four general categories of activity comprising: '(1) providing transitory digital network communications services; (2) system caching; (3) hosting information on service provider servers; and (4) providing information location tools.'[24] Further, according to the nature of liability, some researchers classify above activities into two liability groups. The activities in category (1) and (2) are classified into 'direct liability' group. The activities in category (3) and (4) are classified to the 'vicarious or contributory liability' group.[25]

---

17 The services listed in s512(b)-(d) includes: (b) System caching; (c) storage of information on systems or networks at direction of users; and (d) information location tools.

18 Band, J. and M. Schruers (2002). at 303-304.

19 Fessenden, G. (2002). at 398.

20 Band, J. and M. Schruers (2002). at 303-304.

21 Case Summary: *A & M Records, Inc v. Napster, Inc.* United States District Court for the Northern District of California, 2000 U.S. Dist. LEXIS 6243 (May 5, 2000) [Online] Available: http://www.law.uh.edu/faculty/cjoyce/copyright/release10/AMRecords.html

22 Also see Fessenden, G. (2002). at 398. Fessenden stated: 'The U.S. District Court for the Northern District of California held that, "Because Napster does not transmit, route, or provide connections (for allegedly infringing music files) through its system, it has failed to demonstrate that it qualifies for the 512(a) safe harbor." Napster's activity did not qualify as a conduit of transitory communications.'

23 Napster did not provide MP3 download service directly via its own network, but provided this service indirectly via Internet. So it loses the ISP immunity in section 512(a).

24 Band, J. and M. Schruers (2002). at 304. See s512(k)(1) of the DMCA. The definition of a service provider for purposes of the safe harbour for providing digital network communications services is somewhat narrower. See also, s 512(a)-(d) of the DMCA.

25 Holmes, L. H. (2001) at 234-238

Specifically, the safe harbour provision in section 512(a) limits ISP liability for providing 'transitory digital network communications' services. It immunizes ISPs that are acting as mere conduits for information from the liability of the third party.[26] Section 512(b) limits ISP liability for 'system caching. It provides immunity for the ISPs that intermediately or temporarily store 'material on a system or network', as part of managing network performance, for the purposes of improving network efficiency.[27] While Section 512(c) limits ISP liability for 'hosting information on service provider servers' at the direction of end users. Bretan gave some examples of functions in this safe harbour category including the storage of user home pages, Usenet and auction site postings, and chat rooms.[28] Lastly, section 512(d) offers a safe harbour for ISPs that 'provide information location tool', such as 'directory, index, reference, pointer, or hypertext link'.[29] These tools may link users to other websites indiscriminately[30], even link to an 'online location containing infringing material or infringing activity'[31].

In a word, to receive the protection in the 'ISP safe harbours', ISPs must ensure the activities they conducted fall within above four categories (in section 512 (a)-(d) of the DMCA) first.

Conditions for Eligibility & Their Applications

Conditions for Eligibility

In order to obtain the benefit of the limitations on liability in ISP safe harbour of DMCA, first the ISP must qualify as a 'service provider' and the conducted activities must be in the scope of safe harbour protection (introduced above). Second, the provider must satisfy two overall conditions:[32]

(1) The ISP must adopt, implement, and inform users of a policy

---

26 A 'transitory digital network communication' here means 'transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider' at the initiation of third parties.(s 512 (a)(1) of the DMCA). It also includes the ISP's intermediate or transient storage of that material in the course of such transmitting, routing, or providing connections. For more details, see Bretan, J. (2003). 'Berkeley Technology Law Journal Annual Review of Law and Technology Intellectual Property Copyright: Digital Media - Harbouring Doubts about the Efficacy of s 512 Immunity under the DMCA.' in 18 *Berkeley Technology Law Journal* 43 at 48-49.

27 For example, when ISPs manage their networks, they may intermediately or temporarily store certain material for the purposes of 'reducing network congestion generally and speeding access to popular sites'. See Bretan, J. (2003) at 49. See also 3 Melville B. Nimmer & David Nimmer, Nimmer on Copyright § 12B.03[A] (2002)

28 See Bretan, J. (2003) at 50.

29 Section 512(d) of the DMCA.

30 Holmes (2001) at 236.

31 Ibid

32 Band, J. and M. Schruers (2002) at 304 and Also see section 512 (i)(1)

providing for the termination of repeat infringers.

(2) The ISP must also accommodate 'standard technical measures' used by copyright owners.[33]

After that, ISP must make sure it also meets the conditions specified in section 512 (a)-(d). Put simply, to receive the benefits in the safe harbour provision of s 512 (a) (on 'transitory digital network communications'), an ISP must ensure meet the following requirements:

(1) the transmission was initiated by the user and not the ISP;
(2) the ISP does not select the transmitted material;
(3) the ISP does not select the recipients of the material;
(4) the material is not stored by the ISP for a period longer than necessary for the transmission of the material; and
(5) the ISP does not modify the content of the material.[34]

To receive the benefit in safe harbour provision of s 512 (b) (on 'system caching'), an ISP must meet the following requirements:

(1) the content of the retained material must not be modified;
(2) the provider must comply with rules about 'refreshing' material — replacing retained copies of material with material from the original location— when specified in accordance with a generally accepted industry standard data communication protocol;
(3) the provider must not interfere with technology that returns 'hit' information to the person who posted the material, where such technology meets certain requirements;
(4) the provider must limit users' access to the material in accordance with conditions on access (e.g., password protection) imposed by the person who posted the material; and
(5) any material that was posted without the copyright owner's authorization must be removed or blocked promptly once the service provider has been notified that it has been removed, blocked, or ordered to be removed or blocked, at the originating site.[35]

Moreover, to receive the benefits of safe harbour provisions of ss 512 (c)

33 By virtue of section 512(i)(2) of the DMCA, 'Standard technical measures' means technical measures that copyright owners use to identify or protect copyrighted works, that have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair and voluntary multi-industry process, are available to anyone on reasonable nondiscriminatory terms, and do not impose substantial costs or burdens on service providers.

34 See U.S. Copyright Office, 'The DMCA of 1998 - U.S. Copyright Office Summary', [Online] Available: http://www.loc.gov/copyright/legislation/dmca.pdf, at 9.

35 Ibid at 10.

and (d) (on 'hosting information' and 'providing information location tool'), an ISP must satisfy the following conditions:

(1) the ISP must respond expeditiously to remove or disable allegedly infringing material if it receives sufficient notice;
(2) the ISP must lack actual knowledge or awareness of facts or circumstances from which infringing activity is apparent; and
(3) the ISP must not receive a financial benefit directly attributable to the infringing activity, if the ISP has the right and ability to control such activity.[36]

Applications of Conditions in the DMCA Regimes

As to application of above conditions, the conditions listed in section 512 (a) are relatively easy to understand and apply. The article will next focus on examining the applications of those conditions listed in sections 512 (b)-(d) in the DMCA regimes, particularly their application in 'notice and takedown regime'.

Notice and Takedown Regime

In *RIAA v Verizon Case*, Chief Judge Ginsburg summarised the 'notice and takedown regime'. She stated:

> Notably present in ss 512(b)-(d), and notably absent from s 512(a), is the so-called notice and take-down provision. It makes a condition of the ISP's protection from liability for copyright infringement that 'upon notification of claimed infringement as described in [s 512] (c)(3),' the ISP 'responds expeditiously to remove, or disable access to, the material that is claimed to be infringing.

Under the DMCA, if the activities that ISPs conducted fell into categories in section 512(b)-(d), and the ISPs want to receive the benefits of immunity, then they must 'institute systems of notice and takedown by which copyright holders can identify infringing material for ISP removal'.[37]

Under this system/regime, first, the ISP must designate an agent to handle infringement claims. The agent's main duties include receiving notification of the storage of infringing files on its service from copyright owners and listing the procedures that copyright owners must follow in notifying the ISP about any unauthorized material.[38] Moreover, for the purpose of easing the burden on the copyright owner, the DMCA requires ISPs must make their agents' names and contacts readily available both through the ISPs' own website and through

36 Band, J. and M. Schruers (2002) at 304. also see s 512 (c)(1), (d) of the DMCA.
37 Bretan, J. (2003) at 50. Through these procedures, the DMCA has set up explicit roles/liabilities for all parties (ISPs, copyright holders and subscribers).
38 Berger, S. (2001) at 102, also see s 512 (c)(2)-(3) of the DMCA.

registration with the Copyright Office.[39] Secondly, to notify the agent of infringing activity, the aggrieved party (copyright holder) shall submit a formal notice to the ISP's agent. In order to be an effective notice, a written communication must contain specific identifying elements required in s512(c)(3) of the DMCA.[40] Substantial compliance with the notice requirement is essential. If the notice submission from copyright owners is not complete, the ISP may not have a duty to disable access to the allegedly infringing material.[41] Lastly, once an ISP becomes aware of any infringing materials stored on its network (for example, the ISP received the copyright holder's notice), it must act expeditiously to remove or otherwise disable access to the files in order to qualify for this safe harbour.[42]

Indeed, the 'expeditiously taking down' procedure is good for immediately preventing an online copyright infringement. However, these procedures may also cause the problem of 'wrongful takedown'. As such, in order to reduce the risks of pre-adjudicated/wrongful takedown, the DMCA provides that 'the ISP cannot be liable for good faith taking the identified material down', and even allows the ISP to replace the removed or disabled material in certain circumstances.[43] The DMCA also provides an analogous 'counter notification procedure' whereby a subscriber can challenge the infringement claim. By virtue of s 512 (g) (2)and (3), in certain circumstances, an ISP may 'replace the removed material and ceases disabling access to it not less than 10, nor more than 14, business days following receipt of an effective counter notice'.[44]

In addition, under some circumstances,[45] an ISP may still qualify for safe harbour even if it fails to remove access after notice,[46] for example when the removal 'imposes substantial costs on the ISP or substantial burdens on its systems or networks' (see s512(i)(2)(c)).

From above provisions, we can see the intention of the DMCA trying to establish strong incentives for the ISP and copyright owners to work together in

---

39 Bretan, J. (2003) at 51, also see s 512 (c)(2)(A)-(B) of the DMCA.

40 See section 512 (c)(3)(i)-(vi). The elements of effective notification include: 1) a signature of a person authorized to act on behalf of the owner of the copyright allegedly infringed; 2) identification of the work infringed or a representative list of such works if multiple works exist at a single site; 3) identification of the infringing material and information sufficient to allow the ISP to locate it; 4) contact information of the complaining party; 5) a statement of good faith; 6) a statement of accuracy of the claim under penalty of perjury.

41 Fessenden, G. (2002) at 399. Also see s 512 (c)(2) of the DMCA.

42 Sections 512(c)(1)(A)(iii), (c)(1)(C) of the DMCA.

43 See s 512(g)(1)-(3) of the DMCA.

44 Also see Folawn, C. (2003) at 991-992 'If the ISP actually ends up removing the material from a user's account or domain, the ISP is immune from liability, provided that it takes reasonable steps to notify the user about the takedown, gives *counter notice* to the copyright holder should the ISP replace the material in question, and replaces the material within fourteen days following receipt of the counter notice.'

45 Section 512 (i)(1)and (2) of the DMCA.

46 Fessenden, G. (2002) at 399, also see s 512 (i)(2)(c) of the DMCA.

detecting and dealing with online copyright infringements,[47] and trying to achieve better a balance for all parties in copyright law.

Knowledge Test

In order to be immune from liability, it is also essential that the ISP has 'no actual or constructive knowledge' of the infringement and the infringing material exists on the network at the sole direction of users.[48] Specifically, this provision may require that:

(1) the ISP does not have actual knowledge that the material/activity is infringing;
(2) in the absence of such actual knowledge the ISP is not be aware of facts or circumstances from which an infringing activity is apparent; or
(3) if the ISP obtains such knowledge or awareness, the ISP acts expeditiously to remove or disable access to the material;[49]

In practice, usually an effective notice submission under the DMCA scheme will satisfy the ISP's 'actual knowledge requirement' for the alleged infringement, and thereby obliges the ISP immediately to take down the infringing material.[50] In addition, the DMCA seems also to provide another method for identifying 'actual knowledge' – the existence or otherwise of actual knowledge is to be 'tested by a reasonable person'. Fessenden said in 2002, by virtue of section 512(c), 'it is determined that an ISP has 'actual knowledge' if the infringing material would be apparent to a 'reasonable person' operating under

47 Mercurio, B. (2002). 'Internet Service Provider Liability for Copyright Infringements of Subscribers: A Comparison of the American and Australian Efforts to Combat the Uncertainty.' Murdoch University Electronic Journal of Law Volume 9(Number 4), [online] available: http://www.murdoch.edu.au/elaw/issues/v9n4/mercurio94nf.html#n33 at Paragraph 19.

48 Folawn, C. (2003) at 990-991, also see s 512 (c) of the DMCA

49 Section 512(d)(1)(A)(B)(C) and S 512(c)(1)(A)(i)(ii)(ii) of the DMCA. In other words, an ISP will be denied safe harbour, if it has actual knowledge that the material/activity is infringing, or has actual knowledge of facts or circumstances from which the presence of infringing activities would be apparent, and thereafter has failed to remove expeditiously or disable access to the infringing activity.)

50 See Fessenden, G. (2002) at 399, especially see note 56 of that article: 'Sen. Rpt. 105-190 (1990); Hendrickson, 165 F. Supp. 2d at 1089, 60 U.S.P.Q.2d at 1340 (C.D. Cal. 2001) (explaining that the DMCA expressly provides that if the copyright holder's attempted notification fails to "comply substantially" with the elements of notification described in subsection (c)(3), that notification "shall not be considered" when evaluating whether the service provider had actual or constructive knowledge of the infringing activity under the first prong set forth in s 512(c)(1)of the DMCA).'

the same or similar circumstances'.[51]

No Control and Direct Financial Benefits Requirement

In addition to complying with notice and take down procedures and actual knowledge requirement, the safe harbour provision also requires that an ISP 'have little benefit and control over the infringement'.[52] The DMCA explicitly provides that to receive the immunity of the ISP safe harbour, the ISP must 'not receive a financial benefit directly attributable to the infringing activity, in a case in which the service providers has the right and ability to control such activity'.[53] (See s 512(c)(1)(B); and s 512(d)(2) of the DMCA.)

A typical example about the application of this requirement may be the *Napster Case*. Napster maintained a central server database and provided a living dictionary (a link list that enables its subscribers to downloading unauthorized MP3 files). Therefore it had a certain level of control over its subscribers. Moreover, by providing such a service, Napster could have the opportunity to get benefits from advertisers, subscribers, and music downloads. As such, it is not hard to understand why the court finally held that Napster did not qualify for safe harbour protection.[54]

In summary, if ISPs can meet all above requirements, then they will obtain the large, sweeping immunity of the ISP safe harbour in the DMCA, including monetary, injunctive and equitable relief.

Evidence Collection & Subpoena Procedure

As Bretan said, while ISPs may qualify for immunity, the safe harbour provisions do not protect those end users who use an ISP's facilities to infringe copyrighted works.[55] However, it is often hard for copyright owners to collect the evidence of online copyright infringement (it is especially hard to detect the identity of ISPs' subscribers who conduct infringing activities) without the cooperation of the ISPs. Therefore, in addition to limiting the liability of ISPs, OCILLA establishes a procedure by which a copyright owner can ask a district court to issue a subpoena requiring the ISP to disclose the identity of the alleged primary infringer.[56]

According to s512(h)(2), an effective request must include a copy of a

---

51 Id at 400, also see section 512 (c)(1)(A)(i)of the DMCA.

52 S 512 (d) (2)-(3) of the DMCA.

53 S 512(c)(1)(B) s 512(d)(2)of the DMCA.

54 There are also other reasons causing the Napster not qualified for ISP safe harbour protection, such as it failed to meet the definition of 'service provider' in the DMCA. See Fessenden, G. (2002) at 398.

55 Bretan, J. (2003) at 52.

56 Section 512(h)(1) of the DMCA, also see The Digital Millennium Copyright Act of 1998 - U.S. Copyright Office Summary [online] available: http://www.loc.gov/copyright/legislation/dmca.pdf , at 9.

notification described in section 512(c)(3), a proposed subpoena, and a sworn declaration that the information sought will only be used for the purpose of protecting copyright. Upon receipt of the issued subpoena, an ISP must expeditiously disclose the identity of the alleged infringing subscriber, regardless of whether it has determined that the content in question actually violates copyright.[57] Otherwise, the ISP will fall out of the protection of the ISP safe harbour and be subject to the corresponding liabilities.

However, s 512 (h) does not provide an explicit scope for applying such a subpoena. In particular it does not answer whether this subsection applies to an ISP acting only as a conduit for data transferred between two internet users, such as persons sending and receiving e-mail or sharing P2P files, and leaves this to the court to decide. Nevertheless, in December 2003, the U.S. Columbia Circuit Court examined both the terms of § 512(h) and the overall structure of § 512 in the *Verizon Case*, and explicitly concluded 'a subpoena may be issued only to an ISP engaged in storing on its servers material that is infringing or the subject of infringing activity'.[58] Based on this conclusion, the court ruled that subpoenas issued by the Recording Industry Association of America (RIAA) under the DMCA seeking the identity of individuals engaging in peer-to-peer file sharing of copyrighted works were invalid,[59] and remanded this case to the district court to vacate its order which had enforced the said subpoena.

Policing Infringement v. Protecting Privacy

The DMCA also contains a provision to ensures that ISPs are not placed in the dilemma of choosing between losing the ISP safe harbour immunity and preserving the privacy of their subscribers. Section 512 (m) explicitly states that 'nothing in section 512 (whole section) requires ISP to monitor its service or access material in violation of law (such as the Electronic Communications Privacy Act) in order to be eligible for any of the liability limitations'.[60] (See U.S. Copyright Office Summary on the DMCA 1998.)

Reading this provision, it is clear that the U.S. congress did not intend to require ISPs to police their services, investigating possible infringements, or make

57 Ibid Also see section 512(h)(5) of the DMCA.

58 *Recording Industry Association of America, Inc (RIAA) v Verizon Internet Services, Inc* , December 19, 2003 [Online], available, http://www.eff.org/Cases/RIAA_v_Verizon/opinion-20031219.pdf , at 7.

59 'E-News December 2003-January 2004', in *Federal Relations E-News 2004*, [Online] Available http://www.arl.org/info/frn/frnmon.html#deccopy

60 The Digital Millennium Copyright Act of 1998 - U.S. Copyright Office Summary [online] available: http://www.loc.gov/copyright/legislation/dmca.pdf , See also DMCA section 512 (m)(1)-(2).

difficult judgments as to whether conduct is or is not infringing.[61] The same position was also upheld by the U.S. Court. In *Ellison v Robertson Case* (2002), [62] the court rejected the plaintiff's argument that section 512(i) requires an ISP to police its system for potential infringement.

Some Comments

Advantages of the ISP Safe Harbour Provisions

In general, the DMCA and its ISP safe harbour provisions have offered ISPs affirmative defences whereby they can escape liability for copyright infringement acts conduced by third parties, whether facing direct, vicarious, or contributory liability.[63] It has also basically achieved the dual purpose of limiting the liability of ISPs for copyright infringement and protecting copyright from unauthorized online distribution. The achievement of this purpose can be credited to the clear and specific procedures established in the DMCA and the ability of legislators to balance the interests of all parties through these procedures.

Specifically, on one hand, the DMCA contains very specific provisions for limiting ISP liability. Especially, section 512 (introduced above) not only specified the scope of the ISP safe harbour but also clarified the specific conditions and exemptions for applying these provisions. These specified provisions do assist parities' understanding of the law.[64] It also facilitates the enforcement and implementation of ISP safe harbour provisions.

On the other hand, the DMCA is trying to establish strong incentives for the ISP and copyright owners to work together in detecting and dealing with online copyright infringements.[65] It is always trying to balance the benefits of all the stakeholders (parties). Such an intention can also be found in its safe harbour provisions. For example, in section 512, the 'requirements on designating ISP agent', 'expeditiously taking down' provisions and 'subpoena procedures' are designed for protecting copyright owners' interests. These provisions enable copyright owners to detect quickly and yet inexpensively, and to remove unauthorized materials from the Internet. They also make it easier for copyright

---

61 Such an intention has been achieved in DMCA by allowing ISPs that have actual knowledge of infringement to receive safe harbour, providing that they expeditiously takes down the infringing material/activities. Also see Fessenden, G. (2002) at 400.

62 See Ellison v. Robertson, 62 U.S.P.Q.2d 1170 (C.D. Cal. 2002), available at 2002 WL 407696. Also see Band, J. and M. Schruers (2002) at 304, esp note 82.

63 Holmes, L. H. (2001) at 234.

64 Mercurio, B. (2002). 'Internet Service Provider Liability for Copyright Infringements of Subscribers: A Comparison of the American and Australian Efforts to Combat the Uncertainty.' in *Murdoch University Electronic Journal of Law* Volume 9(Number 4), [online] available: http://www.murdoch.edu.au/elaw/issues/v9n4/mercurio94nf.html#n33 at Paragraph 32.

65 Ibid, Paragraph 19.

owners to collect evidence / information of suspected infringers, and detect online copyright infringement. The 'counter notification procedure' is designed to balance the benefit of the users/subscribers. It provides a good opportunity for the subscribers to defend themselves, and helps to minimize the risks of 'wrongful takedown'. Section 512 (m) is designed for exempting ISPs' liability on policing its service (investigating possible infringements, monitoring its service). And the exemption provision in section § 512 (i)(2)(c) is designed for reducing economy loss and burden of ISPs on 'wrongful takedown'.

Limits of ISP Safe Harbour Provisions

Limits of the Notice and Takedown Regime

Although the DMCA (and its ISP safe harbour) tries to balance the interests of all stakeholders, it is still very problematic in some areas, even its 'notice and takedown regime'. Indeed, the 'counter notification procedures' provide certain protection for users/subscribers and give them an opportunity to defend themselves, but such an opportunity seems to come too late. 'Expeditiously taking down' provisions in the DMCA often leave no chance for the subscribers to explain, before their materials/activities are terminated or they know such a termination will be conducted.[66] This may greatly increase the risk of 'wrongful takedown', and place ISPs in an embarrassing situation with their clients. They have to face the dilemma: either lose the immunity of the ISP safe harbour or lose (at least offend) their clients.[67]

The misuse of the 'notice and takedown' provisions has incurred widespread criticisms from both ISPs and the public. In *Online Policy Group v. Diebold*, Cohn argued that 'greater checks should be read into the notice-and-take-down/safe harbor provisions of the DMCA', and contended that 'parties that misuse the DMCA's procedures should be liable for damages incurred by those they target'.[68] Moreover, some commentators argue that the misuse of the 'notice

66 Also see Mercurio, B. (2002) para 34, 'Although the content provider, in its complaint to the ISPs, must be specific and clear about what is being infringed, the statute only requires a "good faith belief" that an infringement exists. A "good faith belief" falls short of solid evidence of infringement, therefore the ISP is forced to remove material whenever they receive a complaint or lose its safe harbours'.

67 ISPs are often criticized by their subscribers due to 'wrongfully taking down the subscribers' materials'. Many subscribers believe that their ISPs just caved to the notice of copyright owner and had not even try to defend the rights of their customer. In 'DMCA Takedown Notice, Scientology, and PacBell', the author (end user) complained 'Did SBC (his/her ISP) try to verify that these were copyrighted works? I still have to find out. I honestly highly doubt that they *are* copyrighted works. I imagine SBC just caved in and didn't even try to defend the rights of their customer (me).' See http://www.peerfear.org/rss/permalink/2003/02/04/1044497702-DMCA_Takedown_Notice_Scientology_and_PacBell.shtml.

68 Further, Cohn urged that in determining whether misuse has occurred, 'the court should ask if the party invoking the procedures, after considering possible fair use

and takedown' provisions will challenge the 'free speech' right of the public. They believe these provisions give copyright owners (content providers) an opportunity to 'silence communication and remove material which is not infringing copyright'.[69]

As such, future legislation should provide more protections for ISPs and their subscribers (public users). New legislation should provide an opportunity for subscribers to respond to the claims of a copyright owner, before their files or activities are taken down.

Limits of Subpoena Procedures

The DMCA's 'subpoena procedures' (introduced above) also have some potential problems, especially in terms of the scope of the subpoena's application and subscriber's privacy issues. The subpoena provisions in DMCA are often abused by copyright holders to investigate and gather information that would not generally be available in the off-line world.[70] For example, in *FatWallet* Wal-Mart intended to abuse the subpoena power to obtain non-copyrightable price information from ISP.[71] And in the recent *Verizon* case, RIAA intended to abuse the subpoena power to seek the identity of a Verison subscriber who allegedly used Kazaa peer-to-peer software to share music online.[72] Some commentators were critical of the fact that the RIAA subpoena had related to conduct 'outside the limited scope of the extraordinary subpoena authority' of the DMCA.[73] The same position was also upheld by the U.S. Court. Finally, the court ruled that the subpoena was invalid.

Although the court decision in *Verizon* is in favor of protecting subscriber's privacy,[74] the result was only reached on a technical reading of the statute.[75] In

---

defences, believed that it had a "likelihood of success on the merits" in its claim of copyright infringement--the standard often used by courts in considering injunctive relief.' For more details, please refer to http://cyberlaw.stanford.edu/blogs/ . For more details on *Online Policy Group v. Diebold* , please refer to http://www.eff.org/Legal/ISP_liability/OPG_v_Diebold/.

69 Mercurio, B. (2002) para 34 and 36.

70 Bretan, J. (2003) at 53.

71 For more details, see AScribe Newswire, FatWallet Victorious in Challenge to Wal-Mart's Frivolous Digital Millennium Copyright Act Subpoena, [Online] available: http://www.nyfairuse.org/dmca/wallmart fw.xhtml (Dec. 5, 2002) .

72 For more information, refer to Electronic Frontier Foundation, 2004, *RIAA v. Verizon* Case Archive [Online] Available, http://www.eff.org/Cases/RIAA_v_Verizon/.

73 'E-News December 2003-January 2004', in *Federal Relations E-News 2004*, [Online] Available http://www.arl.org/info/frn/frnmon.html#deccopy.

74 The court concluded 'a subpoena may be issued only to an ISP engaged in storing on its servers material that is infringing or the subject of infringing activity.' *Recording Industry Association of America, Inc (RIAA) v Verizon Internet Services, Inc* , December 19, 2003 [Online], available, http://www.eff.org/Cases/RIAA_v_Verizon/opinion-20031219.pdf , at 7.

fact, the constitutional issues (such as privacy, freedom of expression) were not addressed by the court at all. So it is not a real victory for subscriber's privacy. The court's decision does create more certainty for applying the subpoena provisions to some degree (especially for the users of P2P files sharing software). However, it has not solved all potential problems in subpoena provisions.

In addition, going beyond a simply technical reading of the statute, the court's decision seems to have more implications. In the *Verison* case, Chief Judge Ginsburg stated:

> …We are not unsympathetic either to the RIAA's concern regarding the widespread infringement of its members' copyrights, or to the need for legal tools to protect those rights. It is not the province of the courts, however, to rewrite the DMCA in order to make it fit a new and unforseen internet architecture, no matter how damaging that development has been to the music industry or threatens being to the motion picture and software industries…
> …The plight of copyright holders must be addressed in the first instance by the Congress; only the "Congress has the constitutional authority and the institutional ability to accommodate fully the varied permutations of competing interests that are inevitably implicated by such new technology."…

This statement showed that the US court had also identified the problems existing in current DMCA provisions. And the court has decided to leave all these issues to the Congress, and believe it is a duty of the Congress to reform legislation (amend DMCA) and provide better solutions for these complex issues in current DMCA, such as how to achieve a good balance between effectively preventing online copyright infringement and protecting subscriber's privacy.

Summary

In summary, the DMCA has provided a good model for helping other countries (for both common law and civil law countries) to establish their own ISP safe harbour regimes, but it is not perfect and still has some potential problems that need to be solved by future legislation.

---

75 As Miller said, 'The result was reached on a technical reading of the statute, and turned on the fact that a subpoena can only be sent if a DMCA notice-and-takedown letter can also be sent. A DMCA notice-and-takedown letter can only be sent to the ISP if the ISP can remove access to the material (and not if the only way to remove access is to terminate a user's account). Thus, a copyright owner cannot send a DMCA notice-and-takedown to an ISP for what a user shares via P2P (the ISP can do nothing but terminate the user's account, which is not a remedy under a DMCA notice-and-takedown letter). Consequently, if no notice-and-takedown may be sent, no subpoena may be issued.' Also see Ernest Miller, '*Verizon Wins Against DMCA Subpoena*', [Online] Available, http://importance.typepad.com/the_importance_of/2003/week51/

Japan's ISP Safe Harbour

In this section, the article will examine the ISP 'safe harbour' legislation in Japan. First, it will briefly review the history of Japan's ISP legislation. Then it will examine the scope and conditions of its ISP safe harbour, and provide some comments, particularly focusing on Japan's 'seven day notice and takedown regime' and its heterogeneous approach.

History of the Legislation

In order to implement the new requirements of the WIPO Internet Treaties, the Japanese government amended both the Copyright Law and the Unfair Competition Prevention Law ('UCPL'), and introduced the anti-circumvention provisions to its legislation in 1999.[76] Further, in 2001, the Japanese government established its own ISP safe harbour legislation and provides 'specified telecommunications service providers' with immunity from damages liability for the unlawful activities of their subscribers.[77]

Horizontal Approach

In essence, the new legislation outlines a list of ISP safe harbours almost identical to those provided by Title II of the DMCA, and Article 14 of the E.U. E-Commerce Directive. It follows a 'horizontal approach' similar to that of the E.U.[78]

Put simply, a significant difference between the U.S. 'vertical approach' and the 'horizontal approach'[79] is the comparative breadth of the safe harbour

---

76 Also see: 'II. History of Copyright Systems in Japan' in 'Copyright System in Japan' [online] available: http://www.cric.or.jp/cric_e/csj/csj.html. The Copyright Law Amendments prohibit the distribution of devices that circumvent technological measures that protect copyright and related rights (copy control measures). The UCPL prohibits the distribution of devices that circumvent access control measures. Also see: http://www.meti.go.jp/english/report/data/gCD1103e.html 'Amendment to the Unfair Competition Prevention Law (Draft)', by Ministry of International Trade and Industry (March 1999).

77 Katoh, M. (2002). 'Intellectual Property and the Internet: A Japanese Perspective in Symposium: Legal Regulation Of New Technologies: Protection, Privacy, And Disclosure; Panel 1: Anti-Circumvention Measures, License Restrictions, And The Scope Of IP Protection: Protection From Copying Or Protection From Competition.' In 2002 *Journal of Law, Technology and Policy* 333, at 340. Also see 'History of Copyright Systems in Japan' [online] available http://www.cric.or.jp/cric_e/csj/csj.html [last visit 30/10/2003].

78 Ibid.

79 Holmes, L. H. (2001) at 237-238. This creates a unified, 'horizontal' approach to determining the extent of Internet provider liability in Europe, and avoids the uncertainty of having different legal standards for determining when ISPs face potential liability.

provisions. The ISP safe harbour provisions of the United States DMCA only apply to the ISPs under copyright law, but ISP safe harbour provisions in the E.U. Directive will apply to all areas of law involving ISP. [80]

Since Japan takes the 'horizontal approach', Japan's ISP safe harbour also applies equally to all unlawful conduct. It can not only be applied in copyright issues, but can be applied also in defamation, indecency and many other legal issues (in which ISPs participate).[81]

Scope of Safe Harbour & Conditions for Eligibility

Japan's ISP safe harbour mainly comprises two parts: (1) the immunity from 'liability to the person harmed by the unlawful content'; and (2) the immunity from 'liability to the subscriber'. Like the DMCA, Japan's Safe Harbour provisions also provide specific conditions for ISPs receiving the immunity in the safe harbour.

Under Japan's Safe Harbour provision, in order to receive the benefit of immunity from liability to the person harmed by the unlawful content, an ISP must satisfy the following conditions:[82]

(1) the ISP did not know that the right of another person would be infringed by the distribution of the content;
(2) there was no sufficient ground for finding that the ISP could have known that the right of another person would be harmed by the distribution; or
(3) the ISP was not the sender of the information.

Moreover, to obtain immunity from liability to the subscribers, an ISP must terminate its subscriber's unlawful online contents in two situations:[83]

(1) when the ISP had 'good ground sufficient' to believe that the right of another person would be wrongfully infringed due to the distribution of the content; or
(2) when the ISP
    a receives a notice from the harmed person that the content is harmful;
    b forwards the notice to the subscriber; and
    c within seven days, does not receive an explanation from

80 Ibid Holmes 'Unlike OCILLA's limiting provisions, which provide safe harbors for Internet providers only under copyright law, the EU Directive will apply across the board to all areas of law involving ISPs.' Also see Rosa Julia-Barcelo, On-Line Intermediary Liability Issues: Comparing E.U. and U.S. Legal Frameworks, 2000 Eur. Intell. Prop. Rev. 22(3) at 108.
81 Katoh, M. (2002) at 340.
82 Katoh, M. (2002) at 341.
83 Ibid at 341.

the subscriber of why the content is not unlawful.[84]

Through these provisions, we can see that Japan has established a 'notice and takedown regime' with its own features ('seven day notice and takedown regime'), for the purpose of quickly detecting and stopping the online copyright infringement.

Unlike the U.S. scheme in the DMCA, Japan's 'seven day notice and takedown' regime provides a chance for a subscriber to explain and respond to the claims from copyright owners, before the ISP terminates its files/activities. A formal notice from the harmed person (e.g., the copyright owner) itself will not satisfy the ISP's 'actual knowledge requirement' for the alleged infringement. However, if the subscriber fails to provide a satisfactory explanation (within seven days), and the ISP does not remove the content (after the 'seven days'), then the ISP will find it very hard to assert that it does not have sufficient grounds to believe that the content is unlawful, and may therefore fall out of the safe harbour.[85]

In addition, there are some exemptions from the 'seven day notice and takedown regime'. In order to terminate expeditiously the online infringement and to circumvent the seven day period during which the service provider must wait for the subscriber's response, major associations of ISPs and copyright owners have produced a 'voluntary guideline'. The guideline specifies a kind of special notice from the copyright holder or credibility certification organization that would enable the ISP to take down immediately the claimed files/activities of subscribers.[86]

As such, legislation and industry guideline working together makes Japan's 'notice and takedown regime' more complete. It also means ISPs can make different responses to claimed online infringement according to different circumstances.

Some Comments

In comparison with the U.S. legislation, like the counterpart of the U.S. DMCA, Japan's ISP safe harbour legislation (especially its 'seven days notice takedown regime') not only provides ISPs with an opportunity to receive the immunity from liability for the infringing acts of their subscribers, but also creates a mechanism by which a copyright holder can require a ISP to remove infringing

84 It should be noted that major associations of service providers and copyright owners have also agreed to a voluntary guideline that can '*circumvent the seven day period'* during which the service provider must wait for the subscriber's response. For more details, refer to 'Knowledge Test' section in this article.

85 Katoh, M (2002) at 341.

86 Ibid Katoh stated, "the guidelines specify the kind of notice from the rights-holder or credibility certification organization that would provide the service provider with 'grounds sufficient' to take down the content without waiting seven days for the subscriber's response."

material from the Internet.

Unlike the 'notice and takedown regime' of the DMCA, Japan's 'seven days notice takedown regime' seems to provide more protection for the interests of subscribers. It provides subscribers with an opportunity to respond to a copyright holder's allegations prior to removal of the allegedly infringing material. Under Japan's regime, ISPs do not have to terminate the files/activities of subscribers immediately just because they receive a formal notice from the harmed person (e.g., the copyright holder).

On the other hand, Japan's voluntary guideline of industries (introduced above) provides some specific circumstances in which ISPs can take down the claimed infringement directly without waiting seven days for the subscriber's response. By providing copyright owners a more immediate and 'the U.S. style' protection, it reduces the risk of the subscriber abusing the 'seven days period' to harm the interests of copyright holders.

In summary, this article believes Japan may serve as an example for other countries to avoid simple solution and pursue more heterogeneous approaches.[87] The Japanese government does not regard adapting/expanding copyright legislation as the single solution. It also tries to use industries guidelines, other legislation (e.g. competition law), and the 'horizontal approach' of the E.U, and makes all of them work together to deal with the new issues in the digital era (including the ISP issues).

Australia's Situation and Recommendations

As part of the core of this article, section four will review the development of Australia's ISP legislation, especially the new requirement (in terms of ISP liability) under the Australia-United States Free Trade Agreement (FTA). Then, it will examine the 'ISP safe harbour' in current Australian copyright law, and try to explore its potential problems and provide some specific solutions. Some most recent cases of the Australian music industry will be examined.

History of the Legislation

In accordance with its obligations under the WIPO Internet Treaties, Australia enacted the *Copyright Amendment (Digital Agenda) Act* 2000 ('DAA') to address the threats posed to digital intellectual property by rapid developments in technology.[88]

---

87 Also see Katoh, M. (2002) at 337. Japan believes it should try to '*avoid the easy solution of expanding intellectual property rights'*. It believes that 'substantive changes to the law will not, by themselves, transform Japan into a leading IP-based nation. Rather, Japan must pursue a more heterogeneous strategy.'

88 Gamersfelder, L. (2002). "Digitizing copyright law: an Australian perspective" in *Commercial Law Quarterly* (December 2001- February 2002): at 3. However, some commentator believes Australia's DAA has not met all the requirements in the WIPO Internet treaties of 1996 yet. One commentator in DRM Watch Staff website said, '…

In enacting the DAA, the Australia government intended to achieve dual purposes: addressing concerns of copyright owners; and providing greater certainty about ISP responsibilities to copyright owners.[89] Like the counterpart of the U.S. DMCA, the DAA also included an ISP safe harbour provision for both defining and limiting the direct, authorization liability[90]of ISPs for online copyright infringement.

The DAA has now been in force for nearly three years, and has been the subject of its first three-year review. In April 2003 the Attorney-General appointed the law firm Philip Fox to conduct a major part of the Government's broader review of the digital agenda reform. And ISP liability (Carrier and carriage server provider's liability) has become one of main issues in this review.[91]

New Requirements in the FTA

At the beginning of this year (on 8 February 2004), Trade Minister Mark Vaile concluded an agreed text for the Australia-United States Free Trade Agreement (FTA) with his US counterpart, Trade Representative Bob Zoellick. As Allens Arthur Robinson suggested, the conclusion of this Agreement has 'major implications for the sectors of the Australian economy and society that focus on intellectual property, telecommunications, media, entertainment and electronic commerce'.[92] This FTA includes a special chapter for Intellectual Property Rights (IPR)[93] and provides many specific requirements about strengthening IPR protection.

As to ISP liability in the FTA, the U.S. statement explicitly requires Australia to 'provide rules for the liability of ISPs for copyright infringement, reflecting the balance struck in the U.S. DMCA between legitimate ISP activity

---

the greater issue is that Australia had heretofore not adopted copyright legislation that brings the country into line with the WIPO copyright treaties of 1996, on which both DMCA and the European Copyright Directive (EUCD) are based.'

89 Mercurio, B. (2002) in paragraph 65.

90 Also called 'vicarious or contributory liability'

91 The scope of the Digital Agenda Review will look at issues which include, (1) Library and archives and educational copying; (2) Carrier and carriage server providers liability; (3) Technology protection measures, circumvention devices and rights management; (4) Rights issues (including first digitisation and temporary copying); (5) Piracy issues arising from use of new technologies, for example, CD burners and peer-to-peer software. For more details, see Philip Fox Law Firm website [Online] Available: http://www.phillipsfox.com/whats_on/Australia/DigitalAgenda/DigitalAgenda.asp

92 Allens Arthur Robinson, 2004, Australia-United States Free Trade Agreement: impacts on IP, communications and technology, [Online] available: http://www.aar.com.au/pubs/ip/foftafeb04.htm or http://www.aar.com.au/pubs/pdf/ip/foftafeb04.pdf

93 See Chapter 17 of Australia-United States Free Trade Agreement, [Online] Available: http://www.dfat.gov.au/trade/negotiations/us_fta/text/index.html

and the infringement of copyrights'.[94] As such, new legislation would be obviously more favourable to copyright holders and place more obligations on ISPs.[95]

Reading the ISP section of the FTA, readers will find that it is just like a 'simplified version' of ISP safe harbour provision in the Title II of the United States' DMCA. The Draft of the ISP liability section not only requires Australia to introduce a regime requiring ISP compliance with right holders' requests if an ISP wants to obtain immunity for the infringing actions of its subscribers (the U.S. Notice and Takedown Regime),[96] but also requires Australia to provide 'avenues for content owners to subpoena ISPs for information about ISP users who are suspected of using the services to store unauthorized material' (the U.S. Subpoena Procedures).[97]

As introduced above, if Australia accepts whole ISP sections drafted in the FTA, that means Australia will import the whole of the U.S. ISP safe harbour. It will also import all potential problems in current U.S. ISP legislation.[98] As such, when Australia reforms its DAA (import the U.S. DMCA regime as the FTA required), it should be very mindful of the problems in DMCA, and work out its own solutions.

ISP Safe Harbour Provisions in the DAA

Before making any suggestions for Australia's legislative reform, it is necessary to examine its current ISP legislation first. Unlike the United States' DMCA approach, Australia took a 'broad statement of authorisation principles combined with the express limitation of liability in certain circumstances' approach to regulate the ISP liability.[99] The DAA defined and limited the liability of ISPs in relation to both 'direct' and 'authorization' liability for the copyright infringement on the Internet.

In general, the DAA only imposes liability on an ISP in two situations:

---

94 Office of the United States Trade Representative, 2004, Trade Facts: Free Trade 'Down Under' - Summary of the U.S.-Australia Free Trade Agreement in (February 8, 2004), Washington, DC [Online] available: http://www.iprsonline.org/resources/docs/2004-02-08-ustr-australia.pdf .

95 Allens Arthur Robinson, 2004, Australia-United States Free Trade Agreement: impacts on IP, communications and technology, [Online] available: http://www.aar.com.au/pubs/ip/foftafeb04.htm or http://www.aar.com.au/pubs/pdf/ip/foftafeb04.pdf .

96 Ibid.

97 DRM Watch Staff, 'Free Trade Agreement Brings New Copyright Laws to Australia', [Online] Available, http://www.drmwatch.com/legal/article.php/3311921 (February 12, 2004).

98 See section 2.6.2 of this article: 'Limits of (the U.S.) ISP Safe Harbour Provisions'

99 'Exposure Draft and Commentary: Digital Agenda Copyright Amendments - Proposed provisions implementing the Government's decision on the Digital Agenda reforms' at Para 130 [online] available: http://www.sentry.org/~trev/project/edexp.doc. (last visited 3/11/2003).

(1) when the ISP is responsible for determining the content of the communication; or
(2) when the ISP authorizes an inveiglement of the copyright in a capacity other than that of merely providing the facilities for the communication of copyright material.[100]

More specifically, s 22(5) (6), s43A and s111A of the DAA deal with 'direct' infringement of ISPs in category (1). S36(1A), s 101(1A), s39B and s112E of the Act deal with the 'authorization' infringement of the ISP in category (2).

Immunity from Direct Liability

As to immunity to 'direct liability', the DAA provides a safe harbour for the ISPs who do not directly control the content of the communication. Section 22(6) of the DAA provides that 'a communication, other than a broadcast, is taken to have been made by the person responsible for determining the content of the communication'. This means that copyright owners only have remedies against the person who determines the content of the material made available online. In the other words, ISPs will only be subject to direct liability for anything communicated on the Internet if they are responsible for determining the content of the communication.

The DAA also provides immunity for the ISPs who directly conduct temporary reproduction. Specifically, s 43A(1) provides immunity for 'temporary reproduction' of a work or its adaptation as part of the technical process of making or receiving a communication. S 111A (1) provides immunity for temporary copy of audiovisual items as part of the technical process of making or receiving a communication. However, the two defences do not apply in relation to the making of a temporary reproduction or copy of subject matters in the course of communication if the making of the communication is an infringement of copyright.[101]

In addition, the immunities for temporary copies in the DAA also include the browsing of copyright material online,[102] and the reproductions made in the course of some caching.[103]

Immunity for Authorization Liability (Vicarious or Contributory Liability)

As mentioned above, the DAA also provides safe harbour provisions for both defining and limiting ISPs' 'authorization liability' for online copyright

100 Docker, L. (2002). 'The ghost of Moorhouse' in *Media and Arts Law Review* 7(No.2) at 116.
101 Sections 43(A)(2) and 111(A)(2) of the DAA.
102 Thus, it excludes users from liability for browsing unauthorised information. Also see Mia Garlick & Simon Gilchrist, (1999), 'The Digital Age: Will Oz Ever Get There' in 3 *TeleMedia* 6, at 79.
103 Mercurio, B. (2002) paragraph 56.

infringement. In order to assist the court to determine whether an authorization has happened, s 36(1A) and s 101(1A) of the DAA provide an inclusive, non-exhaustive list of factors that an Australian court has to consider, including:

> (a) 'the extent, if any, of the person's power to prevent the infringement;
> (b) the nature of the relationship between the person and the infringer, and
> (c) whether the person took any reasonable steps to prevent or avoid the doing of the act, including whether the person complied with any relevant industry codes of practice.'

As the Revised Explanatory Memorandum stated, these factors codify 'the principles in relation to authorization that currently exist at common law', in particular, 'the principles established by the decision of the High Court in the *Moorhouse case*'.[104] These provisions provide ISPs with 'certainty about their responsibilities to copyright owners and the steps they need to take to avoid infringing copyright'.[105] In comparison with the counterpart of the United States' DMCA, Australia's provisions seem too broad and simple.

In addition, section 39B and section 112E provide some standards for assisting the court to identify 'contributory negligence' and determine whether an 'authorization' had happened. According to the section 39B, a person (including a carrier or carriage service provider) who provides facilities for making, or facilitating the making of, a communication will not be taken to have authorised any infringement of copyright in a work 'merely because another person uses the facilities so provided to do something the right to do which is included in the copyright'. Section 112E applies in exactly the same way to audio visual items.

Moreover, as to the meaning of s 39B, the Revised Explanatory Memorandum of the DAA states:

> New s.39B has the effect of expressly limiting the authorisation liability of persons who provide facilities for the making of, or facilitating the making of, communications. The section provides that such persons are not taken to have authorised the infringement of copyright in a work merely because another person has used the facilities to engage in copyright infringement. For example, a carrier or other service provider will not be liable for having authorised a copyright infringement merely by providing the facilities by which the communication was facilitated.

However, by reading the original words in current s 39B of the DAA, it is not hard to find the meaning of this section (especially the conditions for accessing

104 Docker, L. (2002) at 117.

105 Lau, T. (2002). "*Australia v Napster*: how would Australian courts respond?" in *Australian Intellectual Property Law Bulletin* vol 14(number 10): at 128.

the safe harbour in s39B[106]) seems quite different from the explanation in the Revised Explanatory Memorandum.[107] (This is also one of legislative flaws in current DAA. More details about the inconsistency of these two documents will be introduced later.)

Comments and Recommendations

Attempts for a Good Balance v. Oversimplified Provisions

Like the counterparts in the U.S. and Japan, Australia's ISP safe harbour provisions also try to balance the benefits of all parties, and provide more certainty for ISP.[108] However, oversimplified provisions and lack of specific enforcement procedures make a good balance of all interested parties hard to achieve, and also cause many uncertainties for applying the DAA safe harbour in the practical world.

For example, in the recent *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd case* (*Kazaa* case),[109] partly because Australialacks specific 'subpoena provisions[110]' (like the provisions in section 512 (h) of DMCA), Music Industry Piracy Investigations (MIPI) required the court to issue an 'Anton Piller' order, and raided the ISP's offices themselves for collecting needed information of the ISP's subscribers. This kind of investigation is always conducted by applicants themselves, so the court's order may be abused to collect unauthorized information. Same abuse was also found in Kazaa case and Justice Wilcox said 'it seems likely that some material was taken that fell outside the authority of the Anton Piller orders'.[111] (More details on the *Kazaa* case, 'Anton Piller' orders, and 'subpoena procedures provisions' will be introduced later in section 4.4.3.)

One of main reasons that Australian government prefers its current approach[112] rather than the U.S. approach is that the government believes the

---

106 '…merely because another person uses the facilities so provided to do something the right to do which is included in the copyright' (in s 39B of the DAA).

107 '…merely because another person…. to engage in copyright infringement' (in Memorandum).

108 Such as offer ISPs affirmative defences whereby they can escape liability for subscribers' activities.

109 *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* [2004] FCA 183 (4 March 2004) [Online] Available: http://www.austlii.edu.au/cgi-bin/disp.pl/au/cases/cth/federal_ct/2004/183.html?query=%7E%20anton%20piller#disp1 .

110 According to s 512(h) of DMCA, upon receipt of the issued subpoena, an 'ISP' must expeditiously disclose the identity of the alleged infringing subscriber. As such, the information of subscribers will be collected by their ISPs, not by copyright holders.

111 Tony Smith, 'Kazaa fails to overturn music biz data seizure orders' [Online] Available: http://www.theregister.co.uk/content/6/36089.html (8th of March, 2004).

112 As introduced before, unlike the U.S. DMCA approach, Australian government took an 'broad statement of authorisation principles combined with the express limitation of liability in certain circumstances' approach to regulate the ISP liability.

use of an DMCA approach would 'add an unnecessary level of complexity' to the DAA.[113] Before the DAA enacted, Australia did examined the ISP safe harbour provisions in the DCMA and also believed these provisions provide 'a high degree of certainty' for ISP. However, the government believes the 'certainty' is only credited to the 'detailed approach' of the U.S. - 'a set of very detailed and complex provisions'.[114] In fact, the establishment of such a 'certainty' is not just due to the specificity and complexity of these provisions'. It more depends on the complete enforcement mechanisms created by these provisions,(such as its 'notice and takedown regime').[115] It is these regimes/mechanisms that clarified the roles which all interested parties should play, and established strong incentives for the ISPs and copyright holders to work together in detecting and dealing with online copyright infringement.

Nowadays importing the U.S. ISP liability regimes has become one of important requirements of the FTA. The Australian Copyright Council had also declared that they support 'the introduction of procedures for notice and takedown of copyright material by ISPs' into Australian copyright law'.[116] As such, it seems that the door for establishing Australian own 'Notice and Takedown Regime' is open now.

Clarifying Confusions & Establishing Australian Notice and Takedown Regime

There is a confusion about the meaning of 'reasonable steps' in the Authorization Test Provisions - s 36(1A)(c) and s 101(1A)(c) of the DAA.[117] Owing to lack of specific enforcement mechanism/regime, the DAA does not directly answer what 'reasonable steps' should be taken to prevent or avoid the

113 'Exposure Draft and Commentary: Digital Agenda Copyright Amendments - Proposed provisions implementing the Government's decision on the Digital Agenda reforms' at Para 130 [online] available: http://www.sentry.org/~trev/project/edexp.doc. (last visited 18/3/2004).

114 Ibid, Para 129.

115 In the other words, a good enforcement mechanism is more important than the complex provisions. For example, Japan's provision is not as complex and detailed as that of the U.S. However, it provides a good balance for the interests of all parties and is easy to enforce, because it also established a (the U.S. style but not exactly same) enforcement mechanism (*'seven-day notice and takedown regime'*).

116 This declaration was made in January of 2003. See Australian Copyright Council, 2003, Submission on proposed free trade agreement with the United States [Online] Available: http://www.copyright.org.au/PDF/Submissions/X0203.pdf .

117 In order to determinate whether there is authorization, s 36(1A) and s 101(1A) of the DAA provides an inclusive, non-exhaustive list of factors that a Australian court has to consider, including:

(a) the extent, if any, of the person's power to prevent the infringement;
(b) the nature of the relationship between the person and the infringer, and
(b) whether the person took any reasonable steps to prevent or avoid the doing of the act, including whether the person complied with any relevant industry codes of practice.

infringement, if ISPs want to receive the immunity in the ISP safe harbour provisions.[118]

This article suggests that Australia should establish its own enforcement regime - Australia's 'Specified Seven-Day Notice and Takedown Regime' to clarify the confusions and solve the problems in current DAA. Australia can incorporate the main framework of the DMCA 'notice and takedown system' with Japan's 'seven days notice and takedown regime' and create a new regime with its own features. And the new regime will be expected to provide greater certainties for all interested parties and even achieve a better balance than the United States' DMCA.

Specifically, first Australia can apply its 'notice and takedown regime' to protect copyright holders' interests, and allows them, inexpensively and quickly, to remove materials that they believe is infringing from the Internet. Second, Australia can take Japan's 'seven days notice' approach and provide the subscribers with an opportunity (seven-day period after they receive the takedown notice) to respond to a copyright holder's allegations before their ISPs remove their materials.[119] Third, Australia can also provide some exemptions for 'seven-day period'. It can provide some specific circumstances in which ISPs can immediately take down the claimed infringement materials, and circumvent the 'seven-day period' during which the ISP must wait for the subscriber to respond to the notice of the alleged infringement.[120] These circumstances/exemptions can either be explicitly stated in the DAA or specified in an industry guideline. Lastly, like the DMCA, Australia can provide some specific situations in which an ISP may still qualify for safe harbour even if it fails to remove access after notice.[121]

Under such a specific enforcement mechanism (proposed above), it will be much easier to answer whether an ISP has taken a 'reasonable steps' in s 36(1A)(c) and s 101(1A)(c). First, if the subscriber fails to provide a satisfactory explanation (within seven days), and the service provider does not remove the content (after the 'seven days'), definitely the ISP will find it very hard to assert that it has taken 'reasonable steps' to prevent the infringement. Second, if the claimed infringement is within the exemptions for the 'seven-days approach'[122] but a ISP fails to take down promptly the claimed materials/activities, then the ISP will not be held to have taken a 'reasonable step'. Third, if a takedown action will

---

118 As Mercurio said, '*It would seem this would mean removal of the infringing material, but could it mean simply sending a letter to the subscriber asking for the material to be removed or even investigating and removing the material only when it has been found to be infringing'* see Mercurio, B. (2002) at para 65.

119 The ISPs do not have to terminate the files/activities of subscribers just because they receive a formal notice from the harmed person (e.g., the copyright holder) within seven days period.

120 These provisions can reduce the risk of the subscriber abusing the 'seven days period' to harm the benefits of copyright holders.

121 'In some cases, an ISP that fails to remove access after notice can still qualify for safe harbor if the removal imposes substantial costs or substantial burdens on their systems or networks.' Fessenden (2002) at 399. Also see s 512 (i)(2)(c) of the DMCA.

122 It is under the circumstances in which the ISP has to immediately takedown.

cause their huge economy loss and burden, and an ISP satisfies the specific exemptions for whole 'notice and takedown regime', then the 'reasonable step' will not be an issue in that case.

Another potential problem in current DAA is about ISP liability for 'wrongful takedown'. As Mercurio has critically noted, unlike the counterpart of the U.S., the DAA 'is silent on the extent of ISP liability for removing non-infringing material and leaves undefined any recourse resulting from a wrongful takedown'.[123]

To solve this problem and strengthen the protection to ISPs, this article suggests, first, the new regime should ensure the ISP 'cannot be liable for good faith taking [down]', and allow the ISP to replace the removed or disabled material in certain circumstances.[124] Second, the new DAA should also directly provide ISPs' some specific exemptions from whole 'notice and takedown regime', such as exempt ISPs' liability when an expeditiously takedown action will cause their huge economy loss and burden.[125]

In addition, under the new regime, Australia may also adopt America's 'counter notification procedures' to minimize the risks of 'wrongful takedown' and protect the benefit of subscribers. The counter notification procedure would clarify the measures that a subscriber can take when he finds his files had been wrongfully taken down.

Lack of Subpoena Procedures & Recent Cases of Australia Music Industry

In some recent cases in Australia, by virtue of the 'Anton Piller' order obtained from court, copyright holders raided the offices of ISPs directly to collect ISP subscribers' information for the purpose of detecting online copyright infringement. Owing to a lack of subpoena procedures, it seems that Australian copyright holders are attempting to use 'Anton Piller' orders as an alternative of subpoena provisions in s 512 (h) of DMCA.

In the most recent case of *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (the *Kazza* case), the Music Industry Piracy Investigations (MIPI) raided 12 premises pursuant to an 'Anton Piller' order.[126] The raids targeted Australian-based operations of Internet file-sharing network Kazaa.[127]

123 Mercurio, B. (2002) at para 66.

124 See Part II 'U.S. ISP safe harbour: Section 3.2 b of this paper: under the subtitle '(c) Expeditiously Taking down, Replacement and Exemptions' also see s 512(g)(1)-(3) of the DMCA.

125 Of course, these exemptions should be subject to a set of specific circumstances.

126 Kazza Case: *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* [2004] FCA 183 (4 March 2004) [Online] Available: http://www.austlii.edu.au/cgi-bin/disp.pl/au/cases/cth/federal_ct/2004/183.html?query=%7E%20anton%20piller#disp1.

127 Jennifer Dudley, Recording giants raid university computers (February 07, 2004), [Online] Available: http://www.couriermail.news.com.au/common/story_page/0,5936,8603150%255E953,00.html .

Beside the offices of Sharman Networks (owners of the Kazaa peer-to-peer file sharing software), Telstra and three universities were also raided.[128]

The action of the MIPI has provoked criticism. One commentator has argued that it is improper to allow applicants themselves to enter the respondents' premises for the purpose of collecting evidence, which might be applied by the applicants in litigation to charge the respondents.[129] The commentator said:

> The reason I find this so note worthy is WHO did the raiding. … The thing that disturbs me is that it is the organization ITSELF that does that raiding! ….that just opens up a large can of worms that is completely unnecessary. You're letting what is basically the accuser perform the search and seizure, which introduces a level of bias and probably vindictiveness that shouldn't be present during these types of actions.

Although this commentator seems mix up 'Anton Piller orders' provisions in Australia,[130] which can be applied in pre-trial procedures for purpose of collecting evidence, with 'subpoena procedures' provisions in the section 512 (h) of United States DMCA, indeed the 'Anton Piller'order 'is essentially unfair to the accused party'[131] and may be abused by applicants to collect unauthorized information (as introduced in section 4.4.1[132]).

As such, future legislation of Australia should provide an explicit scope for the applications of 'Anton Piller Order' and 'Subpoena Procedures', so that the

---

128 Are We There Yet? Music Piracy in Australia [Online] Available: http://www.futureviperowner.com/archives/000103.htm (February 06, 2004).

129 Ibid.

130 The investigators (who directly collect evidence) are the ISPs under the 'subpoena procedures' of the DMCA, while the investigators in 'Anton Piller' order are often the applicants themselves. Moreover, unlike the 'Subpoena Provisions' in the DMCA, 'In British and British-derived legal systems, an Anton Piller order (frequently spelt as Anton Pillar order) is a court order which provides for the right to search premises without prior warning. This is used in order to prevent the destruction of incriminating evidence, particularly in cases of alleged copyright infringement.' – from Wikipedia Encyclopedia [Onlien] Available: http://en.wikipedia.org/w/wiki.phtml?title=Anton_Piller_order&printable=yes , Also see *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* [2004] FCA 183.

131 Ibid 'The first such order (Anton Piller order) was issued in the case of *Anton Piller KG vs Manufacturing Processes Limited* in 1976. Because such an order is essentially unfair to the accused party, Anton Piller orders are only issued exceptionally, when (1) there is an extremely strong prima facie case against the respondent, (2) the damage, potential or actual. must be very serious for the applicant, and (3) there must be clear evidence that the respondents have in their possession incriminating documents or things and that there is a real possibility that they may destroy such material before an inter partes application can be made'.

132 The abuse of Anton Piller orders was also found in the *Kazaa* case and Justice Wilcox said 'it seems likely that some material was taken that fell outside the authority of the Anton Piller orders'. (See section 4.4.1 of this article).

applicant can easily tell which information he/she can collect, and identify the right person who has the authority to collect relevant information. (Under an Anton Piller order, the right persons should be the copyright holders. Under a subpoena, the right person should be the ISPs.)

In addition, since in the *Verizon* case the court had explicitly concluded 'a subpoena may be issued only to an ISP engaged in storing on its servers material that is infringing or the subject of infringing activity',[133] Australia may consider explicitly writing such a conclusion into new legislation (codify the court's decision) when importing the U.S. subpoena procedures provisions. This will also create more certainty for the application of subpoena procedures.

This article does not expect all problems can be solved in one time. Regarding other complex issues in subpoena provisions, such as how to achieve a good balance between effectively preventing online copyright infringement and protecting subscriber's privacy, this article suggests that these matters be left to Congress and future legislators to decide.

Confusion in s 39B & Non-exhaustive/Exhaustive Solution

As introduced above,[134] s39B of the DAA specified some conditions for ISP accessing the safe harbour immunity for authorization liability. However, the explanation in the Revised Explanatory Memorandum (the Memo) to this section seems to go beyond the original meaning of this section in the DAA. As to the application of this immunity, s 39B states 'a person … will not be taken to have authorised any infringement … "merely because another person uses the facilities so provided to do something the right to do which is included in the copyright"'. But the Revised Explanatory Memorandum explicitly states that '…persons are not taken to have authorised the infringement … merely because another person has used the facilities to engage in copyright infringement'.[135]

It is clear that the protection scope of the Revised Explanatory Memorandum is much broader than that of the current DAA. As such, some commentator argues 'it must be asked what the legislators intended by inserting the words "to do something the right to do which is included in the copyright"'.[136] Indeed, whether the legislators intend to provide a wide protection for ISP (as was

133 *Recording Industry Association of America, Inc (RIAA) v Verizon Internet Services, Inc,* December 19, 2003 [Online], available, http://www.eff.org/Cases/RIAA_v_Verizon/opinion-20031219.pdf , at 7.

134 Also see section 4.2.2 of this article - 'Contributory Negligence in s39B and s112E'

135 *Revised Explanatory Memorandum* of Copyright Amendment (Digital Agenda) Bill 2000, at para 60, [online] available: http://parlinfoweb.aph.gov.au/piweb/view_document.aspx?ID=560&TABLE=OLDEMS

136 Docker, L. (2002). 'The ghost of Moorhouse' in *Media and Arts Law Review* vol. 7 (No.2) at 119 to 120. Further, Docker said 'those works must mean that the protection is not afforded to a carrier or carriage service provider if the person using their facilities is doing so to communicate material which is in breach of copyright. So when does an ISP lose the Protection of s 39B and s 112E?' S112 E has same problems with s 39B.

explained in the Memorandum) or not, they should make it explicit in the DAA, and try to keep the consistency of the DAA and its explanatory documents.

The new DAA can try to clarify the meaning of clause 39B and rewrite it by more explicit language. It can either provide ISPs an explicit exemption like 'Explanatory Memorandum' stated[137] or provide a narrower protection by attaching some more specific conditions. For example, the new DAA would provide certain specific circumstances in which the ISPs may receive the immunity of safe harbour in s 39B.

Moreover, as a more general solution, Australia can also establish an 'inclusive, non-exhaustive list' in its legislation to specify the main activities ('qualified Internet services') which may receive the immunity of ISP safe harbour. Australia does not have to make a U.S. style 'exhaustive activity list' (in s 512(a)-(d) of the DMCA)[138], since Government believes too specific provisions 'would not easily accommodate future developments in technology'.[139] To other activity which is outside of the proposed 'non-exhaustive activity list' (proposed above), the new DAA may leave it to the court's discretion to decide whether the immunity of ISP safe harbour is available to it.

Horizontal approach & Consistency with Other Legislations

This article does not suggest that Australia should take a 'horizontal approach' to address the ISP protection issues. But it does suggest that Australia should pay more attention to prevent the possible inconsistencies among different legislation or legal documents when drafting new legislation.[140] For example, the legislators should note whether the definition of ISP in the DAA is consistent with the definition in the Broadcast Services Amendment (Online Services) Act 1999 ('BSAA').

This article also suggests that the government should learn from successful experiences of other relevant legislation (even other domestic legislation). For example, the *Broadcast Services Amendment (Online Services) Act*

---

137 '… such persons will not be taken to have authorised the infringement of copyright in a work "merely because another person has used the facilities to engage in copyright infringement"'. See *Revised Explanatory Memorandum of Copyright Amendment (Digital Agenda) Bill 2000*, at para 60.

138 As to *qualified Internet Services*, Safe Harbour of the DMCA limits ISP liability for four general categories of activity including: (1) providing transitory digital network communications services; (2) system caching; (3) hosting information on service provider servers; and (4) providing information location tools, e.g., search engines. For more details, see section 2.2 of this paper.

139 '*Exposure Draft and Commentary: Digital Agenda Copyright Amendments - Proposed provisions implementing the Government's decision on the Digital Agenda reforms'* at Para 130 [online] available: http://www.sentry.org/~trev/project/edexp.doc. (last visited 3/11/2003).

140 For example, as discussed before, in relation to the conditions of accessing the safe harbour, the provision in s39B of the DAA seems quite different from the explanation given in the *Revised Explanatory Memorandum*.

1999 (the DSAA) has outlined 'notification and takedown procedure' resulting from offensive material being posted on the Internet.[141] It sets up a regime whereby Australian ISPs are required to 'take reasonable steps' to 'prohibit access to/remove X rated/Refused Classification material and limit access to R-rated material to people over 18 years old'. The regime in the DSAA looks like an analogue of 'notification and takedown procedures' in the U.S. DMCA. Although 'the regulation of material in that Act cannot be imparted to copyright infringements',[142] it may serve as a good example for establishing a similar 'enforcement regime' in future DAA. By contrast, the proposed new regime in this article ('Australian seven day notice and takedown regime', introduced above) can also serve as an example for the future reform of the BSAA.

More Heterogeneous Methods

Australia should try to avoid simple (single) solution, and pursue more heterogeneous methods in its future copyright legislation reform.[143] In fact, Australia has made certain attempt for a heterogeneous solution, although it might not be a successful attempt. Section 36(1A)(c) of the DAA tries to combine the DAA with the Internet Industry Association of Australia's Code of Practice to 'provide certainty and liability avoidance to ISPs'.[144] However, many commentators have critically noted that this industry code has nothing to do with 'copyright' and said 'the Act's reference to the Code can only be due to oversight and ignorance'.[145] As such, when future legislators attempt to take a heterogamous solution, they should pay more attention to keep a consistency between different legislation and relevant industries rules.

This article suggests, besides adapting current copyright law, Australia should also widely adapt/apply other relevant legislation (e.g. competition law), industries guidelines, IP policies and all possible methods, and make them work together to deal with the new legal issues in the digital era (including ISP protection, free speech on the Internet, online privacy, and many other issues). This article also believes copyright law cannot and also do not have to solve all said problems by itself. For example, regarding online privacy issue, it may be a better solution if we leave it to privacy law or constitution law to deal with.

---

141 Mercurio, B. (2002) at para 65.

142 Ibid Mercurio said, 'The regulation of material in that Act cannot be imparted to copyright infringements… as that Act specifically only deals with RC/X rated content.'

143 As introduced above, Japan may serve as a good example. Besides adapting its copyright law, Japan adopted other legislation , voluntary industries guidelines , and the 'horizontal approach' of the E.U., and made them work together to deal with the new digital challenges.

144 Mercurio, B at para 60.

145 Ibid As Mercurio stated '…the Code of Practice does not even contain the word "copyright." The Code is designed to handle defamation and pornography problems, not copyright infringement….'

Conclusion

This article has introduced and compared the ISP safe harbour provisions in the U.S. and Japan. It has examined both the advantages and the limits in their legislation, in order to seek to learn lessons from their experiences. The article also introduced Australia's ISP safe harbour provisions, and pointed out the potential problems in current DAA by referring to some most recent cases in Australia. It also provided some specific suggestions for Australian future legislation reform under the context of the WIPO Treaties and the Australia-United States Free Trade Agreement (FTA).

In the end, this article would like to adopt and expand an enlightening view from a U.K. IPR Commission Report: the interest of a nation is only best served by tailoring its intellectual property regimes to its particular economic and social circumstances.[146]

As such, when reforming its legislation/policy and importing the US regime, Australia must have a good understanding of potential problems in both Australia's DAA and the United States' DMCA. The reform of the DAA should be based on the current Australian situation, and should be consistent with Australia's development policy, trade need, legislative development, and juridical practices.

146 In developing this paper the author has been enlighten by a particular opinion in a U.K. IPR Commission Report. In Chapter 8, this report states: 'The implication of our analysis is that the interests of [developing countries] are best served by tailoring their intellectual property regimes to their particular economic and social circumstances.' This article believes such a conclusion (in the report) is also applicable for developed countries (all countries in the world). For more details on the U.K Report, refer to Commission on Intellectual Property Rights, 'Report of the Commission on Intellectual Property Rights: Integrating Intellectual Property Rights and Development Policy', London, September 2002 [Online] Available: http://www.iprcommission.org/ .