Building Safe Harbours in Choppy Waters – Towards a Sensible Approach to Liability of Internet Intermediaries in Australia

Peter Leonard considers safe harbours for internet intermediaries in both the Copyright Act and the Broadcasting Services Act, and equivalent provisions in the United States, European Union and certain other jurisdictions.

There has been extensive academic and copyright practitioner analysis of the application of copyright law to internet service providers and internet users in the U.S.A., European Union, Australia, Canada and other major jurisdictions. This debate has been passionate and polarised. Occasionally the debate has descended into trading of slogans between content owners and internet access service provider (**ISP**s), enflamed by some of the more extreme pronouncements of the 'internet should be free' brigade. The online copyright piracy debate in Australia was recently enlivened by debate as to the reasoning of Mr Justice Cowdroy in the action initiated by thirty-four film and television production companies, under the coordination of the Australian Federation Against Copyright Theft (**AFACT**), against the ISP iiNet Ltd for authorisation of acts of copyright infringement by users of iiNet subscribers' accounts.[1] That debate was further fuelled by criticisms as to secondary liability provisions of negotiating drafts of the proposed multi-lateral Anti-Counterfeiting Trade Agreement.

Clause 91 does not appear to have been subject to significant judicial consideration in Australia.

There have also been detailed commentaries as to the operation of content laws in relation to Australian internet access service providers and the Federal Government's proposal for mandatory provider side internet filtering.[2]

Scope of this paper

Given the range of analysis of copyright liability of internet intermediaries and the operation of content laws in relation to internet access service providers, the focus of this paper is elsewhere: instead, we focus on an area that is intriguing for its want of study in Australia: the operation of the limited safe harbours for internet content hosts and for internet service providers provided by Schedule 5 clause 91(1) of the Broadcasting Services Act 1992 (Cth), which states as follows:

> 91(1) A law of a State or Territory, or a rule of common law or equity, has no effect to the extent to which it:
>
> (a) subjects, or would have the effect (whether direct or indirect) of subjecting an Internet content host to liability (whether criminal or civil) in respect of hosting particular Internet content in a case where the host was not aware of the nature of Internet content; or
>
> (b) requires, or would have the effect (whether direct or indirect) of requiring, an Internet content host to monitor, make inquiries about, or keep records of, Internet content hosted by the host; or
>
> (c) subjects, or would have the effect (whether direct or indirect) of subjecting an Internet service provider to liability (whether criminal or civil) in respect of carrying particular Internet content in a case where the service provider was not aware of the nature of the Internet content; or
>
> (d) requires, or would have the effect (whether direct or indirect) of requiring, an Internet service provider to monitor, make inquiries about, or keep records of, Internet content carried by the provider.[3]

Clause 91 does not appear to have been subject to significant judicial consideration in Australia. So far as the author is aware, analysis as to the operation of clause 91 has been very limited and generally as incidental coverage within general reviews of the operation of the Broadcasting Services Act 1992 (Cth).

The lack of study as to clause 91 is interesting for a number of reasons.

Firstly, the provisions is built upon a concept of "awareness", a term without a body of judicial interpretation, unlike the concept of knowledge as extensively analysed in many statutory and common law causes of action. By contrast, the broad safe harbour under U.S. Federal law, section 230 of the Communications Decency Act of 1996,[4] has been considered in numerous judicial decisions[5] and

1 Roadshow Films v iiNet (No. 3) [2010] FCA 24. There are many analyses of the decision: see for example, David Brennan, ISP liability for copyright authorisation: the trial decision in Roadshow Films v iiNet, Melbourne Law School Legal Studies Research Paper No. 475; also Part One: Communications Law Bulletin, volume 28, no 4 April 2010, Part Two: Communications Law Bulletin, volume 29, no 1 June 2010; Universal Music Australia Pty Ltd v Sharman License Holdings Ltd [2005] FCA 1242 (Wilcox J); Universal Music Australia Pty Ltd v Cooper [2005] FCA 972 (Tamberlin J); Cooper v Universal Music Australia Pty Ltd [2006] FCAFC 187 David Lindsay, Liability of ISPS for End-User Copyright Infringements (2010) 60 Telecommunications Journal of Australia 29.1

2 See Catharine Lumby, Leila Green and John Gartley, Untangling the Net: the Scope of Content Caught by Mandatory Internet Filtering, December 2009, available at http://www.cci.edu.au/publications/untangling-net-scope-content-caught-mandatory-internet-filteriing; David Vaile and Renee Watt, Inspecting the Despicable, Assessing the Unacceptable, Telecommunications Journal of Australia Vol. 59 No. 2 (2009), p27.1.

3 The full text of clauses 90 and 91 of Schedule 5, and related definitions, appears below in Part 9 of this paper.

4 Available at http://www.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000230----000-.html.

5 David S Ardia, Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity under Section 230 of the Communications Decency Act, Loyola of Los Angeles Law Review Winter 2010 Vol 43:473. David Ardia identified and analysed 184 reported decisions from 140 cases between the effective date of section 230, February 1996, and 30 September 2009, in which a party to the proceedings or the Court raised section 230 as a defence to online liability or acts.

the divergence between non-copyright safe harbours and copyright safe harbours for internet intermediaries may be increasing

academic treatise.[6] The comparable provisions at the European Union level, Articles 14 and 15 of the Directive on electronic commerce (2000/31/EC)[7] has been the subject of much less extensive academic treatment or judicial analyses, but there is a significant body of material related to the interpretation of the Directive for statutory drafting to implement the Directive in the twenty seven EU member States.

Each of these safe harbours are expressed in markedly different terms and operate in quite different ways. Clearly the Australian safe harbour falls away once an internet intermediary becomes aware as to "particular internet content": without doubt, "aware" as to its existence, but not necessarily "aware" that the content is infringing, leaving difficult questions as to when and how an internet content host or an internet service provider should take steps to determine whether content is infringing. The policy approach of section 230 of the Communications Decency Act of 1996 is to provide a broad safe harbour, notwithstanding awareness both as to existence and as to the infringing nature of relevant third party content. This is markedly divergent from the 'notice and take-down' procedure in respect of copyright material in the U.S.A. pursuant to the U.S. Federal Digital Millennium Copyright Act[8] (**DMCA**) of 1998 and comparable provisions under Australian copyright law.[9] This radically different approach to infringement of copyright and to other causes of action under U.S. law is not followed in the European Union, where the safe harbour is broadly expressed but dependent upon no "actual knowledge of illegal activity or information knowledge" of the internet content cost or service provider, then leaving EU Member States in their statutory implementation of the Directive to elaborate upon those words, with markedly different outcomes between some Member States.

Clause 91 sits uncomfortably within these divergent approaches, without any expressed policy rationale for its limited scope of coverage or its different approach to that adopted under Australian copyright law. The divergent approaches in national jurisdictions is increasingly problematic given the global availability of internet content and marked national differences in content laws. Moreover, the divergence between non-copyright safe harbours and copyright safe harbours for internet intermediaries may be increasing as some EU Member States and other jurisdictions including New Zealand consider imposition of 'graduated response' requirements on internet intermediaries.

The fact that there has been little published comment by internet industry players for reform of clause 91 probably reflects more that internet content is generally hosted outside Australia, and specifically in the U.S.A., than any satisfaction as to the operation of clause 91. It is reasonable to speculate that the growth in cloud applications and hosted services may change this perspective, and lead to a much closer consideration as to the adequacy or otherwise of clause 91. In addition, the Australian Government is about to embark upon a comprehensive review of laws relating to the convergence of media, communications and internet. Clause 91 sits largely neglected yet at the centre of that convergence. It is one of the relatively few legislative provisions in Australia to expressly address the activities of internet content hosts and one of the few Federal provisions that appears to 'cover the field' of internet regulation to the exclusion of State and Territory legislation.[10]

For the reasons discussed in some detail later in this paper, clause 91 is remarkably limited in its scope of coverage as compared, in particular, to section 230 of the Communications Decency Act and Articles 14 and 15 of the EU Directive. But before making such comparisons it is first necessary to calibrate our language.

Ruminations about intermediaries

Many international debates as to internet law pass 'like ships in the night': a debate never properly opened and hence never closed because the participants have not first ensured that they are arguing about the same issue. Let us first be clear as to the nature and role of the internet intermediaries under discussion and the differences in exculpatory approaches and rules in major countries.

Internet intermediaries may be relevantly characterised in three groups:

(a) communication conduits;

(b) content hosts;

(c) search service and application service providers.

The first category includes intermediaries that facilitate the physical transport of data across the fixed or mobile network: from the user viewpoint, the internet access service provider with whom they have their account, an ISP that is typically a telecommunications carrier (e.g. Telstra, Optus or Vodafone) or a telecommunications carriage service provider (proving carriage services over telecommunications networks owned and operated by others (e.g. iiNet and AAPT). Of course, many other intermediaries are involved in transporting that content and ensuring that it arrives at the right destination, in particular internet backbone providers such as Verizon and Sprint.

internet intermediaries are properly regarded as intermediaries whenever they do not themselves originate actionable content, or in American terms, do not first 'utter' the relevant 'speech'

The second category of intermediaries are content hosts. These are intermediaries that store, cache, or otherwise provide access to third-party content. While any person could set up a blog or Web site on a home server, few people bother to do so. Most content is stored on or made available from servers operated by private intermediaries, including those operated by well-known brand names like Google and Yahoo! An anonymous 'whistle blower' may speak to the world through a blog-hosting service such as Blogger or BoingBoing, a posting of a video to YouTube or DailyMotion, postings to Wikileaks and so on. Unpopular and frequently actionable content may be shared on social networking sites such as Facebook, Flickr and MySpace. Protests may be organised by using microblogs

6 A good online updated section 230 resource is Jonathan Freiden, Overview of Section 230 of the Communications Decency Act, at http://ecommercelaw.typepad.com/ecommerce_law/2007/06/overview_of_sec.html#ixzz14jl5X6HK.

7 Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:NOT. Useful background to the Directive can be found at http://ec.europa.eu/internal_market/e-commerce/directive_en.htm.

8 ss 201-203, codified as 17 USC §511-513.

9 Discussed below.

10 One of the few other Federal statutes broadly covering the internet is the Internet Gambling Act 2001 (Cth).

such as Twitter. In each of these hosting services the hosting intermediary determines limitations that it elects to impose upon users as to the use of its services through its terms of use, including community policies and upload warnings, and its takedown policies. Frequently these hosting services are otherwise unmoderated or unable to control what is uploaded and initially made available: for example, YouTube receives uploads of over 24 hours of audiovisual content every minute. The quantity of Facebook material is best illustrated by reference to user face time: in August 2010 it was estimated that over 10 percent of total time online of US users was spent on Facebook as compared to 9.6 percent on the Google family of services (Google Search, Gmail, YouTube, Google News, Google Earth and so on).[11]

The above examples all relate to copyright, yet as we have already noted internet intermediaries face a myriad of liability exposures and possible causes of action in respect of actionable content

The third category of intermediaries includes application service providers and search engines. In many ways this is the most challenging grouping because of its diversity. Broadly, these intermediaries facilitate access to content by, among other things, indexing it, filtering it, or formatting it, but do not necessarily host the content themselves. Online examples include Google Search and spam-filtering software. These intermediaries are of vital importance because they allow a user to conveniently find and make sense of the vast amount of information available on the Internet and to direct their time-limited attention to the minute sub-set of information that may be of interest to them. Some searches may use terms that find the applications service providers that facilitate patently illegal activity, including pirates being pirated: for example, a search query on the term "Limewire" on 13 November 2010 revealed as a top result www.limewire.com and at that site the following text was screened over the former Limewire home page:

> LimeWire is under a court order dated October 26, 2010 to stop distributing the LimeWire software. A copy of the injunction can be found here. LimeWire LLC, its directors and officers, are taking all steps to comply with the injunction. We have very recently become aware of unauthorized applications on the internet purporting to use the LimeWire name. We demand that all persons using the LimeWire software, name, or trademark in order to upload or download copyrighted works in any manner cease and desist from doing so. We further remind you that the unauthorized uploading and downloading of copyrighted works is illegal.

Following that permanent injection LimeWire is no longer the application of choice for peer to peer music copying. BitTorrent remains the application of choice for peer to peer copying of audio-visual material. BitTorrent can of course be downloaded from numerous sites, including those operated by BitTorrent itself.

These internet intermediaries are properly regarded as intermediaries whenever they do not themselves originate actionable content, or in American terms, do not first 'utter' the relevant 'speech'. The next question then is whether and in what circumstances those intermediaries, when acting as intermediaries, should be liable in respect of actionable content originated by others, for example:

- BitTorrent as application service provider providing the means by which copyright material (as well as non-copyright material) is located on another users computers and made available to the requesting user;
- a hosting service provider providing the platform at which audio-visual material is made available, including that sub-set of material that (may upon review be identified as) infringing a third party copyright or invasive of privacy;
- an ISP for failing to implement active steps to identify and seek out and stop users that have unusual download patterns that may indicate that the user is a requesting or providing user of content to services such as BitTorrent;
- an ISP for failing to take active steps to assist a copyright owner in identifying, gathering evidence or prosecuting alleged breaches of that copyright owner's copyright by a user of that ISP's services.

The above examples all relate to copyright, yet as we have already noted internet intermediaries face a myriad of liability exposures and possible causes of action in respect of actionable content: random examples (among many) include statutory limitations on securities offerings over the internet and advertising of offering of securities or provision of financial advice, restrictions on advertising or provision of online gaming services and therapeutic substances and alcoholic beverages, suits for invasion of privacy, defamation and contempt, restrictions upon court reporting or publication of names or minors involved in court proceedings, breaches of confidentiality and the tort of negligence. Given this range, why has discussion for infringement of copyright occupied so much of the academic literature as to intermediary liability and so much of the legislative agenda?

It was inevitable that copyright would be one of the first major battlegrounds to define new law in many jurisdictions as to the liability of internet intermediaries

First, there is the acknowledged extent of illegal copying of copyright material around the globe. According to the Eurostat figures released in July 2010 by Ms Viviane Reding, the European Union Commissioner for Telecoms and Media, 60 per cent of 'digital natives' – the generation "ready to apply innovations like web 2.0 to business and public life, whether as podcasters, bloggers, social networkers or website owners" - "have downloaded audiovisual content from the internet in the past months without paying". Twenty eight per cent of the interviewed users apparently stated they would not be willing to pay for the downloaded content.[12]

Secondly, there are very significant business interests and business models at stake: in particular, the continuing decline in sales of recorded music and the rapid rise in availability of valuable audio-

---

11 Eric Sinrod, Face Time: Internet Users Stay on Facebook the Longest, October 12, 2010, http://www.duanemorris.com/articles/facebook_gets_most_internet_face_time_3845.html, citing comScore data. For recent Australian survey data, see Australian Communications and Media Authority (ACMA), Communications report 2009-10 series: Report 1 – Australia in the digital economy: The shift to the online environment 11 November 2010; for U.S. data, a convenient source is the Nielsenwire series at blog.neilsen.com/neilsenwire.

12 Viviane Reding, Digital Europe—Europe's Fast Track to Economic Recovery, The Ludwig Erhard Lecture 2009, Lisbon Council, Brussels, July 9, 2009, p.5 available at http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/09/336; see also Alain Strowel, Internet Piracy as a Wake-up Call for Copyright Law Makers—Is the "Graduated Response" a Good Reply? Thoughts from a law professor who grew up in the Gutenberg Age [2009] WIPOJ No. 1, p7.

visual works, such as television shows and Hollywood movies, on BitTorrent and other peer to peer networks.

Thirdly, the inherently decentralised and fragmentary nature of accessed material on peer to peer networks, and the role of individual users rather than service providers as primary infringers, encourages copyright owners to pursue internet intermediaries such as an ISPs as the principal defendants in infringement proceedings.

Much confusion arise from attempts to apply United States concepts of secondary liability to Anglo-Australian principles of indirect infringement and authorisation

Lastly, there has been the relatively recent rise of user generated hosted content sites hosted by major players such as Google (YouTube), and the semi-public or public parts of Facebook, that may be used (directly contrary to terms of use applying to those sites) by content uploaders for mash-ups and other audiovisual works that incorporate third party copyright material. This new form of copyright infringement by content uploaders poses particular challenges for copyright law in many countries as even recently developed statutory schemes did not anticipate user generated content.

It was therefore inevitable that copyright would be one of the first major battlegrounds to define new law in many jurisdictions as to the liability of internet intermediaries. The Anglo-Australian law of copyright generally found authorisation liability for breach of copyright in two ways:

- by (explicitly) granting approval to do an infringing act, such as by purporting to grant a licence to do the act;
- by (implicitly) sanctioning, approving or countenancing the doing of an infringing act, such as by failing to take steps to prevent the doing of the act where one had power to prevent and ought to have known of the occurrence.

It is useful to compare the Anglo-Australian theory of authorisation liability with the two principles of indirect liability that developed over the course of the 20th century US copyright cases, being contributory and vicarious infringement. Contributory infringement requires knowledge of the infringing activity of another (direct) infringer and inducing, causing or materially contributing to that infringement: sometimes called the 'knowledge prong' and the 'material contribution prong'.[13] Vicarious liability requires the right and ability to stop or limit a direct infringement and a direct financial interest in such infringing activity.

In many areas of law other than copyright there are no clear general principles to guide a distinction between primary and secondary liability – and in some areas of law the distinction does not apply at all. For example, some statutes create an offence to "publish" actionable material and provide no guidance as to who is to be regarded as "publishing", leaving open the question of whether well developed but very expansive concepts of '"publish" in areas such as defamation law should be used as analogies in application of the statute. However, in considering the role of internet intermediaries it is useful to start from the general distinction between primary and secondary actors recognised under many legal systems, including the American legal system. U.S. Federal and State civil and criminal rules impose primary liability in relation to publication of material – collectively referred to as "speech" (echoing the broad U.S. First Amendment freedom of speech concept) - on those who are the primary "speakers". Separately, various and more limited forms of secondary liability is imposed on intermediaries who are not the actual "speakers" but who have some nexus, generally through dissemination of the subject 'speech', to the wrongful acts. For example, in the book world, the speakers may be the author and the book publisher, the intermediaries the printer, the distributor, the logistics provider and the bookstores. Internet intermediaries face a myriad of potential legal claims, both civil and criminal, arising from the content and actions of third parties, include liability under intellectual property laws, privacy laws, obscenity laws, liability for defamation and other torts and anti-discrimination laws, and state tort laws. Secondary liability principles frequently are qualified by requirement of proof as to 'actual knowledge' as to the material being 'wrongful', or other limiting (or in some cases, exonerating) factors.

Each internet safe harbour is an attempt to effect a balance between the protection of a person aggrieved and intermediaries' right to develop technologies and business models that facilitate and enable reproduction and dissemination of digital information

The problem is compounded by jurisdictional questions that arise when 'speech' is 'uttered' far from the original 'speaker', best illustrated by the arcane but important trans-Atlantic debate as whether defamatory material is to be taken as spoken where it is first uttered – the so called 'first publication' rule generally applied in U.S. jurisprudence – or wherever it is published – the so-called 'multiple publication rule'[14] famously applied by the High Court of Australia in the Gutnick[15] decision. Many of the multiple publication cases pre-dated the internet and typically involved at least some conscious decision by some intermediary to make available the 'speech' – a book, a magazine, a television or radio program – in the jurisdiction. The cases generally sought to find a requisite level of intent to 'publish' in the relevant jurisdiction, and sometimes a requisite level of knowledge as to the likelihood that the material in the publication was actionable in that jurisdiction: for example, a book distributor electing to import and market a book containing actionable subject matter in the jurisdiction.[16] These cases are often very difficult to apply to the internet, as is well illustrated by the Gutnick decision: should Dow Jones as publisher of the online edition of The Wall Street Journal be liable in Australia in relation to a story about an Australian merely because a

13 See David Hayes excellent analysis of U.S. cases applying theories if contributory liability and vicarious liability to online service providers in David L. Hayes, Advanced copyright issues on the internet, Fenwick and West LLP 2009, available at http://www.fenwick.com/docstore/Publications/IP/Advanced_Copyright_2009.pdf. .

14 A balanced evaluation is given by the U.K. Ministry of Justice in its consultation paper, U.K. Ministry of Justice, Defamation and the internet: the multiple publication rule: Consultation Paper CP 20/09, September 2009 at pp 9-12, available at www.justice.gov.uk. The coalition agreement between the new Conservatives and the Liberal Democrats in May 2010 on their formation of the new U.K. Government included commitment to overhaul of U.K. defamation law "to protect freedom of speech".

15 Dow Jones & Co, Inc v Gutnick (2002) 210 CLR 575; 77 ALJR 255; 194 ALR 433

16 The cases are well summarised in U.K. Ministry of Justice, Defamation and the internet: the multiple publication rule: Consultation Paper CP 20/09, September 2009 at pp 9-12, available at www.justice.gov.uk.

It is costly for intermediaries to consider contending views as to legality of content or offer dispute resolution procedures to their users. It is far less costly to simply remove content alleged to be actionable at the first sign of trouble, or to decline to carry 'edgy' content at all

handful of viewers of the online version of The Wall Street Journal viewed the journal from internet access devices in Australia?[17] If this was the case, why shouldn't North Korean law equally apply to publication in The Wall Street Journal of criticism of North Korean autocracy when read online by Dear Leader on one of the few sanctioned internet access devices in Pyongyang? Because of the difficulty in applying such cases to the internet, various legislatures responded by the creation of safe harbours, effectively ending the development of the common law in respect of secondary liability or authorisation under various causes of action as it applies to internet publication.

Much confusion arise from attempts to apply United States concepts of secondary liability to Anglo-Australian principles of indirect infringement and authorisation ('sanctioning, approving or countenancing'). This confusion is compounded by two factors. First, although many causes of action are deceptively similar under Australian and U.S. jurisprudence, the exoneration principles or defences are quite different and the overhang of the U.S. First Amendment (freedom of speech) affects many decisions. Second, many of the decisions made each day about whether to take down internet content that has been identified and is alleged to be infringing are made in California by application of principles of U.S. Federal or State law or by projection as to what a 'global common denominator' may be, after special account for special factors (i.e. local laws on criticising their monarch). It is simply impossible for any Californian attorney to give effect of the nuances of secondary liability, indirect infringement and authorisation laws as separately developed for different cause of action in a multiplicity of jurisdictions.

Building safe harbours: why are so many 'safe harbours' so unsafe?

One approach to resolution of the complexities of secondary or indirect liability and multiple causes of action is a broadly based 'safe harbour'.

The term 'safe harbour' has caught on around the globe in relation to a broad array of defences and exonerating provisions for internet intermediaries. Of course, there have long been cause of action specific safe harbours, including common law – the 'innocent dissemination' defence to defamation liability[18] is one of many examples. Each internet safe harbour is an attempt to effect a balance between the protection of a person aggrieved and intermediaries' right to develop technologies and business models that facilitate and enable reproduction and dissemination of digital information. In all cases the safe harbours have drafting deficiencies. These drafting deficiencies typically arise in one or both of two ways. First, a safe harbour generally was the outcome of a political compromise effected after heavy lobbying between rights holders or others and the internet industry. Sometimes the drafting deficiency reflects a political compromise that is reflected in vague or open language. Sometimes the provisions were drafted (or amended in the course of passage) in a hurry or with excessive reference to foreign precedents developed in respect of comparable but materially different foreign statutes, in order to give effect to a treaty or under other pressure of time. For example, the Australian Copyright Act safe harbours were a rushed implementation pursuant to obligations accepted by Australia as a condition to implementation of the Australia United States Free Trade Agreement.[19]

United States courts have consistently held that the mere exercise of traditional editorial functions, such as deciding what content to publish or remove, does not make an intermediary responsible for the content it publishes

An example of a broadly based safe harbour is section 26 of the Electronic Transactions Act 2010 of Singapore,[20] as follows:

> Liability of network service providers
>
> 26 (1) Subject to subsection (2), a network service provider shall not be subject to any civil or criminal liability under any rule of law in respect of third-party material in the form of electronic records to which he merely provides access if such liability is founded on:
>
> (a) the making, publication, dissemination or distribution of such materials or any statement made in such material; or
>
> (b) the infringement of any rights subsisting in or in relation to such material.
>
> (2) Nothing in this section shall affect:
>
> (a) any obligation founded on contract;
>
> (b) the obligation of a network service provider as such under a licensing or other regulatory regime established under any written law;
>
> (c) any obligation imposed under any written law or by a court to remove, block or deny access to any material; or
>
> (d) any liability of a network service provider under the Copyright Act (Cap. 63) in respect of:

17 The new Federal U.S. SPEECH Act (to be codified at 28 U.S.C. §§ 4101-05) provides shields for U.S. authors and publishers by preventing a person who obtains a defamation judgment in a foreign court from enforcing that judgment in the U.S., unless that person makes two showings concerning that judgment. First, the plaintiff must show that that the defamation law applied by the foreign court provided as much protection for freedom of speech and the press as the U.S. Constitution and applicable State laws. The Act further provides that a plaintiff cannot enforce its defamation judgment, unless the judgment is consistent with the Communications Decency Act. Second, the plaintiff must show that the foreign court's exercise of jurisdiction over the defendant complied with U.S. due process requirements.

18 See for example the discussion of the High Court of Australia in Thompson v Australian Capital Television (1996) 186 CLR 574.

19 Division 2AA of the Copyright Act 1968 (Cth), inserted to ensure that "carriage service providers" who take reasonable measures to limit and deter copyright infringement are able to attract the benefit of reduced liability for copyright infringement if they introduce certain policies and procedures.

20 See http://statutes.agc.gov.sg/.

there are two ways in which an intermediary may be put on notice of infringing material on its system: notice from the copyright owner, and the existence of "red flags"

(i) the infringement of copyright in any work or other subject-matter in which copyright subsists; or

(ii) the unauthorised use of any performance, the protection period of which has not expired.

(3) In this section:

"performance" and "protection period" have the same meanings as in Part XII of the Copyright Act;

"provides access" , in relation to third-party material, means the provision of the necessary technical means by which third-party material may be accessed and includes the automatic and temporary storage of the third-party material for the purpose of providing access;

"third-party", in relation to a network service provider, means a person over whom the provider has no effective control.

It will be noted that the safe harbour is in relatively broad terms but does not (now) exonerate copyright infringement. The relevant provision was first enacted as section 10 of the now repealed Electronic Transactions Act 1998 of Singapore and then was not subject to a copyright exception: the copyright exception was later introduced following representations by rights holders and Singapore entering into the Singapore-USA Free Trade Agreement[21]. The copyright safe harbour now appears as sections 193B to 193D and 252A to 252C of the Copyright Act (chap. 63) of Singapore,[22] and broadly reflects the U.S. DMCA approach.[23] Under section 193A of the Copyright Act of Singapore "network service providers" are (relevantly) both a person who provides services relating to, or provides connections for, the transmission or routing of data, and a person who provides, or operates facilities for, online services or network access. The latter appears broad enough to capture hosting service providers, although this is not beyond argument.

As a result Singapore has moved from a general exculpatory provision for internet intermediaries to a bifurcated safe harbours for copyright, broadly based on U.S. DMCA, and the other more general safe harbour for many non-copyright claims.

Of course, the most well known general safe harbour for non-copyright claims is that under the Communications Decency Act. We now turn to consider that 'safe harbour' and contrast it with the DMCA provisions and the European Union Directive provisions that were derived from them.

Section 230 of the Communications Decency Act

The Communications Decency Act of 1996 is the name commonly given to Title V of the (U.S. Federal) Telecommunications Act of 1996, codified at 47 U.S.C. § 230. Section 230(c)(1) provides an extensive immunity from liability for providers and users of an "interactive computer service" who publish information provided by others.

It is sometimes suggested that section 230 should now have a more limited role because of increasing sophistication in technological tools, such as filters, to detect certain illegal or offensive internet content. However, that argument is questionable: technological tools are blunt instruments that are likely to block more content than the intermediary intended and are incapable of exercising judgment. For example, while software may identify certain words or phrases or 'flesh tones' in images, the software cannot determine whether the content in fact is obscene, defames others or invades their privacy: such judgement-based determinations require contextual analysis and, in many instances, additional facts. As a result, the assessment of legal liability by intermediaries still cannot be effectively automated. Imposition of active requirements for an internet intermediary to monitor, or block uploaded content as and when uploaded, may so fundamentally affect the business model for 'free' user generated content services that such services may cease to be commercially feasible and hence cease to be made available.

Graduated response is in the course of implementation in France, Taiwan, and South Korea. Graduated response may also be implemented in the United Kingdom, Canada and New Zealand, although the commitment of the (current) legislatures in each of these jurisdictions is less clear

Also, when intermediaries remove potentially actionable content, they often do so without providing an opportunity for the uploader to contest the removal or blocking. It is costly for intermediaries to consider contending views as to legality of content or offer dispute resolution procedures to their users. It is far less costly to simply remove content alleged to be actionable at the first sign of trouble, or to decline to carry 'edgy' content at all. So any increase in the baseline liability exposure for intermediaries will impact their willingness to carry 'edgy' content or preserve its availability. As David Ardia notes, a "profit-maximizing intermediary likely will choose the mechanism that is least costly, rather than the one that preserves the most speech".

Section 230 provides that "no provider ...of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider".[24] 'Interactive computer service' is broadly defined as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet…. ."[25] The most common interactive computer services are, of course, websites.

---

21 Effective 1 January 2004 and available at http://tcc.export.gov/Trade_Agreements/All_Trade_Agreements/exp_007049.asp.

22 See http://statutes.agc.gov.sg/.

23 See further RecordTV v MediaCorp TV Singapore [2009] SGHC 287, Warren Chik and David Yong, Internet Intermediaries and Copyright Law in Singapore, available at http://www.lawgazette.com.sg/2010-04/feature3.htm

24 47 U.S.C. § 230(c)(1)

25 47 U.S.C. § 230(f)(2)

In 2004, in fulfilment of obligations under the (AUSFTA), the Federal Government enacted a copyright safe-harbour regime modelled on US copyright law

Section 230 "immunity" is lost to the extent that the publisher is an 'information content provider', which is defined as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet."[26] This is construed by reference to the information in issue: a defendant may itself carry on business as an information content provider, but if it is not the person or entity responsible for the creation or development of the information in issue, it is entitled to claim the immunity.

A defendant must satisfy each of the three elements to gain the benefit of the immunity:

- the defendant must be a "provider or user" of an "interactive computer service";
- the cause of action asserted by the plaintiff must "treat" the defendant "as the publisher or speaker" of the harmful information at issue;
- the information must be "provided by another information content provider," i.e., the defendant must not be the "information content provider" of the harmful information at issue.

United States courts have consistently held that the mere exercise of traditional editorial functions, such as deciding what content to publish or remove, does not make an intermediary responsible for the content it publishes. These traditional editorial functions include screening objectionable content prior to publication, as well as correcting, editing, or removing content. Taking an active role in editing content, and encouraging or soliciting others to submit content - including content that is likely to be actionable – has not disentitled defendants to section 230 immunity.

Section 230 immunity is not lost once the publisher is on notice of the allegedly defamatory content.[27] As a result, failure to take down a post, even one that gives rise to liability for the individual who posted it, does not of itself take away the safe harbour for the website owner. In this respect section 230 diverges sharply from U.S. copyright law as implemented through the DMCA 'notice and take down' process. However, one of many cases involving fake profiles on online dating services,[28] a decision of the Ninth Circuit in the case of Barnes v. Yahoo!, Inc., held that section 230 did not pre-empt a claim for promissory estoppel based on a specific promise made by a Yahoo! employee that she would "personally walk the [plaintiff's complaint] over to the division responsible for stopping unauthorized profiles and they would take care of it". The court allowed the promissory estoppel claim to go forward because the Yahoo! employee made this specific promise to the plaintiff, noting however that promises made in a Web site's terms of service—for example, a promise to remove all defamatory content, or in marketing materials, do not create an obligation to remove content; "a general monitoring policy, or even an attempt to help a particular person, on the part of an interactive computer service such as Yahoo! does not suffice for contract liability".

Section 230 has been applied in a broad range of cases: defamation, misrepresentation, negligence, deceptive trade practices and false advertising, privacy torts (including intrusion and misappropriation), tortious interference with contract or business relations and intentional infliction of emotional distress. However, the section expressly excludes from section 230 immunity Federal criminal statutes, intellectual property laws, "any State law that is consistent with section 230" and communications privacy law (but not other laws creating rights of personal privacy).[29]

The amendments also failed to address the interrelationship between the 2004 safe harbour and 2001 provisions

Digital Millennium Copyright Act 1998 (DMCA)

The position under US copyright law is different from that under section 230.

The Digital Millennium Copyright Act 1998 (**DMCA**) amended the US Copyright Act.[30] Part of that amendment was the implementation of a notice-and-takedown regime regarding the liability of internet service providers, explicitly including host providers. Hosting, which is denoted in the DMCA as "residing of information on systems or networks at direction of users", is generally exempted from liability if the respective host provider does not have actual knowledge and, upon obtaining such knowledge or awareness, acts expeditiously to remove the material or to disable access.

Relevant internet intermediaries must comply with two general requirements: to comply with standard technical measures and remove repeat infringers.

To qualify for protection under section 512(c), an intermediary:

- must not receive a financial benefit directly attributable to the infringing activity;
- must not be aware of the presence of infringing material or know any facts or circumstances that would make infringing material apparent, and
- upon receiving notice from copyright owners or their agents, act expeditiously to remove the purported infringing material.

Although an intermediary must not have actual knowledge that it is hosting infringing material or be aware of facts or circumstances from which infringing activity is apparent, it is clear from the statute and legislative history that an intermediary has no duty to monitor its service or affirmatively seek infringing material on its system. However, there are two ways in which an intermediary may be put on notice of infringing material on its system: notice from the copyright owner, and the existence of "red flags". The "red flag" test stems from the language in section 230 that requires

---

26 47 U.S.C. § 230(f)(3)

27 The seminal case establishing this proposition is Zeran v. America Online, Inc 129 F.3rd 327 (4th Cir) 1997, cited and followed in 137 cases of the 140 reported and analysed by David Ardia, op cit.. For a discussion of cases in the Zeran line of authority and two divergent decisions, see Patrick Carome and Colin Rushing, Anomaly or Trend? The Scope of §230 Immunity Challenged by Two Courts, Communications Lawyer Vol. 22 No. 1, Spring 2004.

28 The fake profile at issue in Barnes v. Yahoo!, Inc 570 F.3d 1096 (9th Cir. 2009) was typically offensive: the plaintiff's profile had had been created by plaintiff's ex-boyfriend and contained nude photos of the plaintiff, her personal and work contact information, and statements that she was interested in sex. at 1098.

29 47 U.S.C. §§230(e)(1),(2),(3) and (4).

30 The Online Copyright Infringement Liability Limitation Act 1998 was a portion of the Digital Millennium Copyright Act 1998 amending the Copyright law in Title 17 of the United States Code by insertion of section 512; available at http://www.law.cornell.edu/uscode/17/512.html.

Mr Justice Cowdroy reasoned that there could be no act of authorisation unless iiNet actually provided the 'means' of infringement

that an intermediary not be "aware of facts or circumstances from which infringing activity is apparent".

The "red flag" test contains both a subjective and an objective element. Objectively, the intermediary must be found to have knowledge that the material resides on its system. Subjectively, the "infringing activity must have been apparent to a reasonable person operating under the same or similar circumstances", and then the intermediary fail to act expeditiously to remove the infringing content.

As stated by Judge Stanton in the June 2010 summary judgement in Viacom v YouTube:

> The tenor of the [DMCA] provisions is that the phrases "actual knowledge that the material or an activity" is infringing, and "facts or circumstances" indicating infringing activity, describe knowledge of specific and identifiable infringements of particular individual items. Mere knowledge of prevalence of such activity in general is not enough. That is consistent with an area of the law devoted to protection of distinctive individual works, not of libraries. To let knowledge of a generalized practice of infringement in the industry, or of a proclivity of users to post infringing materials, impose responsibility on service providers to discover which of their users' postings infringe a copyright would contravene the structure and operation of the DMCA. As stated in Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, (9th Cir. 2007):
>
> > The DMCA notification procedures place the burden of policing copyright infringement-identifying the potentially infringing material and adequately documenting infringement-squarely on the owners of the copyright. We decline to shift a substantial burden from the copyright owner to the provider.
>
> That makes sense, as the infringing works in suit may be a small fraction of millions of works posted by others on the service's platform, whose provider cannot by inspection determine whether the use has been licensed by the owner, or whether its posting is a "fair use" of the material, or even whether its copyright owner or licensee objects to its posting.

EU Directive on Electronic Commerce

The European Union Directive on electronic commerce (2000/31/EC) (**E-Commerce Directive**) of 8 June 2000[31] is the most prominent example of a broad 'safe harbour' covering both copyright and other causes of action. However, it is beset with problems of interpretation and application as a result of diverse interpretations of a number of the Directive's provisions in the course of implementation into domestic law by EU member states, and lengthy recitals which can be argued as to narrow interpretation of what otherwise appear to be quite expansive safe harbours.

Relevant Articles include:

> Article 12
>
> 'Mere conduit'
>
> 1. Where an information society service[32] is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:
>
> (a) does not initiate the transmission;
>
> (b) does not select the receiver of the transmission; and
>
> (c) does not select or modify the information contained in the transmission.
>
> 2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.
>
> 3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.
>
> Article 14
>
> Hosting
>
> 1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:
>
> (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
>
> (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.
>
> 2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.
>
> 3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.
>
> Article 15
>
> No general obligation to monitor
>
> 1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.
>
> 2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

The Recitals, however, are less clear:

> (41) This Directive strikes a balance between the different interests at stake and establishes principles upon which industry agreements and standards can be based.

---

31 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML.

32 This is a term of art defined in Art. 1(2) of Directive 34/1998/EC as amended by Directive 48/1998/EC, see also Recitals (17) and (18) of Directive 2000/31/EC.

Clearly the first instance judgement gives significant support to ISPs in an argument that they should not be required to intervene in respect of use by their users of third party peer to peer sites, and runs counter to 'graduated response' proposals

> (42) The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.
>
> ……..
>
> (44) A service provider who deliberately collaborates with one of the recipients of his service in order to undertake illegal acts goes beyond the activities of "mere conduit" or "caching" and as a result cannot benefit from the liability exemptions established for these activities.
>
> (45) The limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it.
>
> (46) In order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned; the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level; this Directive does not affect Member States' possibility of establishing specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information.
>
> (47) Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation.
>
> (48) This Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities.

The hosting exemption is of general application and covers, for example, liability for defamation, breach of confidentiality or privacy, intellectual property infringement, and criminal laws. The stronger view is that a hosting service provider not exercising any oversight or editorial control over posting of content is entitled to rely upon Article 15 exemption, provided they meet the other criteria (e.g. absence of relevant knowledge and prompt action once on notice). However, there remains some debate as to whether the hosting exemption is only available to a hosting service provider that does no more than enable users to store data in a technical sense. If so, a website owner that publishes editorial, as well as user generated, content would not be able to benefit from the hosting defence. Further, there is an argument that Recital 42 of the Directive supports an interpretation that a publisher that benefits from advertising revenue arising out of hosting third party content would not be able to benefit from any immunity from liability.

Even more problematic is the range of interpretation as to Article 14(3), which potentially allows extension of liability of an intermediary beyond knowledge and application of different national concepts of 'knowledge'.[33] Recital 47 of the Directive states that Member States are prevented from imposing a general monitoring obligation on service providers. However, "this does not concern monitoring obligations in a specific case." According to Recital 48, Member States may require hosts to "apply duties of care, which can reasonably be expected….in order to detect and prevent certain types of illegal activities". German courts have decided that in particular cases a host provider's liability is not limited to a notice-and-takedown obligation. For example, in a series of cases the German Federal Court of Justice imposed additional duties on eBay, once a seller had been found to be selling replica Rolex watches by posting them on eBay by using the Rolex brand, to take measures to prevent further infringements in future, if such measures are possible and economically reasonable. The court suggested that eBay could reasonably monitor all future offers of Rolex watches on their platform, for example, by installing specific filter software. By contrast, English courts have rejected attempts of trade mark holders to compel eBay to prevent infringements of their customers. Both the German and English courts purported to applied the Directive as admitted into national law, but the different outcome has been said to flow from different domestic legal principles as to availability of permanent injunctive relief based on prior wrongful action.

The status of Articles 14 and 15 will be tested by two recent referrals to the European Court of Justice (ECJ) from the Belgian Courts in cases brought by the Belgian Society of Authors, Composers and Publishers (SABAM) against the ISP Tiscali (now Scarlet) and the social networking site, Netlog. The ECJ will be required to balance the safe harbours against European privacy rights and a provision in the Information Society Directive[34] that requires Member States to "ensure that right holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right".

As at the date of this paper the European Commission was engaged in a Public consultation on the EU Directive. The period for consultation closed on 5 November 2010. The terms of reference included the interpretation of the provisions concerning the liability of intermediary information society service providers".

Repeat Infringers and Graduated Response

The DMCA requires internet intermediaries to remove repeat infringers. The sufficiency of the DMCA requirement has been extensively discussed across the globe, most recently in the 'three

33 See Thibault Verbjest, Gerald Spindler, Giovanni Riccio and Aurelie Van der Perre, Study on the Liability of Internet Intermediaries, November 2007, and in particular the State by State review of the implementation of the Article 14 (Hosting) and discussion of the obligation to block or remove, pp35/115 – 60/115, available at http://ec.europa.eu/internal_market/e-commerce/directive_en.htm.

34 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0029:EN:HTML, see further http://europa.eu/legislation_summaries/internal_market/businesses/intellectual_property/l26053_en.htm.

strikes and you're out' or 'graduated response' debates. In its more extreme form, 'graduated response' allows for a number of notification letters to consumers warning that they are violating copyright, followed by disconnection, with internet intermediaries being required provide content owners with IP addresses of allegedly infringing users. Graduated response is in the course of implementation in France, Taiwan, and South Korea. Graduated response may also be implemented in the United Kingdom, Canada and New Zealand, although the commitment of the (current) legislatures in each of these jurisdictions is less clear. Although each country has adopted or proposes different systems of graduated response, key characteristics usually are: (1) rights holders monitor P2P networks for illegal downloading activities; (2) rights holders provide internet intermediaries with proof (the level of proof required is itself contentious) of infringements being committed by an individual at a given IP address; (3) informational notices are sent through an ISP to the account holder informing him or her of the infringements and of the consequences of continued infringement and informing the user that content can be lawfully acquired online; and (4) if the account holder repeatedly ignores the notices, a tribunal may take deterrent action, with the most severe sanctions reserved for a court.

Graduated response proposals have been particularly contentious when implementation requires the intervention of an internet access service provider, on the basis that the internet service provider has access to contact details about a user and the ability to pass those details to a copyright owner.[35] Issues raised as to intervention of an internet access provider include:

- user privacy,
- proportionality (should internet access be denied effectively across the full range of internet services in response to a particular form of infringement),
- targeting (if a person with a household is using the internet for a particular illegal activity, should all persons using that internet access in that household be affected?),
- burden upon the internet intermediary, and
- 'slippery slope' (today copyright, tomorrow politically unacceptable material and so on).

In addressing these concerns, the UK government identified a range of less severe sanctions than disconnection to address repeated infringements, including blocking specific sites or protocols, capping the speed of a subscriber's Internet connection or volume of data traffic, and content identification and filtering. The concept is that sanctions of this kind would allow for the avoidance of Internet account termination except in extreme circumstances, and would not impact on other services such as a telephone or cable television service. Some proposals for graduated response endeavour to address these issues: for example, the Canadian 'notice notice' proposal' whereby user details are not passed between the copyright owner and the internet access service provider, but the user is provided with notice by the internet access service provider and warning as to the alleged infringement of the copyright owner's copyright.

In Australia, the copyright safe harbour debate has not progressed at the level of announced Government policy since the Government's Australian Digital Economy: Future Directions[36] paper of July 2009. That paper followed a 'consultation draft' which sought submissions, many of which were critical of the current Australian copyright safe harbour.[37] The final paper of July 2009 noted the range of submissions received and stated that the "Australian Government will consider these submissions and whether the scope of the safe harbour scheme should be expanded to include additional types of online service providers".

It may be that the (now Gillard) Government now awaits outcome of the appeal to the Full Federal Court[38] from the first instance decision of Mr Justice Cowdroy in the iiNet case before determining what is required.

The Australian safe harbours: sections 36(1A) and 101(1A) and Part V, Division 2AA of the *Copyright Act 1968* (Cth)

It is outside the scope of this paper to enter into a detailed examination of the safe harbours under the Australian Copyright Act 1968 (Cth).[39] In any event, the operation of those safe harbours will be the subject of detailed consideration by the Full Federal Court in its reserved and pending (as at 12 December 2010) appeal decision in the iiNet case. That noted, we briefly overview the background to the safe harbours and the judgement to place our discussion of safe harbours more generally fully in context.

The seminal pre-internet case on authorisation liability under Australian copyright law is The University of New South Wales v Moorhouse[40] (**Moorhouse**) which involved photocopiers in university libraries. 'Trap infringing copying' was undertaken on a coin-operated photocopier situated in the library from a copy of book held in the library. The university, by the provision of the photocopier in the library and making available the book as a library holding, was alleged to have 'authorised' the subsequent trap copying. One judge (Gibbs J) emphasised in his reasoning a more control-based (vicarious infringement under US law) approach to justify liability: the power of the University to prevent the infringing act, coupled with failure to take reasonable steps to prevent. Two judges (Jacobs J, with whom McTiernan ACJ agreed) emphasised a more approval-based (contributory infringement under US law) approach to justify liability: the conduct of the university effectively invited users to infringe.

In 2001 there was a codification of the authorisation principles developed in Australian cases culminating in the Moorhouse decision, requiring courts determining liability for authorisation infringement of copyright to have regard to, in addition to any other matters, three particular matters:

- the extent (if any) of the defendant's power to prevent the doing of the infringing act;
- the nature of any relationship existing between the defendant and the person who did the infringing act; and
- whether the defendant took any reasonable steps to prevent or avoid the doing of the infringing act, including compliance with relevant industry codes.[41]

---

35 Note in this regard the contention between the European Parliament, as shown in its adoption on 22 September 2010 of the Gallo Report calling for further sanctions for online copyright infringement, and the position of the European Commission. see http://www.europarl.europa.eu/oeil/file.jsp?id=5817632; the Gallo Report is also available at that address.

36 Available at http://www.dbcde.gov.au/digital_economy/future_directions_of_the_digital_economy/australias_digital_economy_future_directions.

37 Submissions are available at http://www.dbcde.gov.au/digital_economy/future_directions_of_the_digital_economy/submissions.

38 As at 14 November 2010, fully heard and awaiting the judgement of the Full Federal Court.

39 Available at http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/current/bytitle/F02280247B0E4B21CA25775B000FBB07?OpenDocument&mostrecent=1.

40 University of New South Wales v Moorhouse (1975) 133 CLR 1.

41 Copyright Act 1968 (Cth), sections 36(1A) and 101(1A).

Uncertainties as to the scope of operation of clause 91 may rightly be considered to have a chilling effect upon the development of user generated content and social networking sites hosted in Australia

A specific exception to authorisation liability was also created, to the effect that a person who provides facilities for making, or facilitating the making of, a communication is not taken to have authorised any infringement of copyright "merely because another person uses the facilities so provided to do something the right to do which is included in the copyright".[42] This 'mere use of facilities' exception was explained in the Second Reading Speech as follows:

> The amendments in the bill also respond to the concerns of carriers and carriage service providers, such as Internet service providers, about the uncertainty of the circumstances in which they could be liable for copyright infringements by their customers. The provisions in the bill limit and clarify the liability of carriers and Internet service providers in relation to both direct and authorisation liability. The amendments also overcome the 1997 High Court decision of APRA v Telstra in which Telstra, as a carrier, was held to be liable for the playing of music-on-hold by its subscribers to their clients, even though Telstra exercised no control in determining the content of the music played.
>
> Typically, the person responsible for determining the content of copyright material online would be a web site proprietor, not a carrier or Internet service provider. Under the amendments, therefore, carriers and Internet service providers will not be directly liable for communicating material to the public if they are not responsible for determining the content of the material. The reforms provide that a carrier or Internet service provider will not be taken to have authorised an infringement of copyright merely through the provision of facilities on which the infringement occurs. Further, the bill provides an inclusive list of factors to assist in determining whether the authorisation of an infringement has occurred.

In 2004, in fulfilment of obligations under the Australia-US Free Trade Agreement (**AUSFTA**), the Federal Government enacted a copyright safe-harbour regime modelled on US copyright law, now Part V, Division 2AA of the Copyright Act 1968 (Cth). This safe harbour limits civil remedies against a carriage service provider in respect of relevant authorisation infringement to two mandatory injunctions: an order that it takes reasonable steps to disable access to online locations outside Australia; and an order that it terminates a specified customer account. To qualify for this safe harbour, the carriage service provider must (among other things) "adopt and reasonably implement a policy that provides for termination, in appropriate circumstances, of the accounts of repeat infringers".[43]

The provisions are complex, but it is clear that their coverage is limited to "carriage service providers". Hence the 2004 amendments were silent as to the liability exposure of internet content hosts.

The amendments also failed to address the interrelationship between the 2004 safe harbour and 2001 provisions. The net effect was that two rounds of legislative reform produced first, a control-based codification of authorisation (sections 36(1A) and 101(1A)), secondly, an exception to authorisation liability for the providers of communications facilities arising from the facilities' mere use by others (sections 39B and 112E) (but operating with "authorisation" law and defences otherwise unaffected), and thirdly, conditional limitations upon copyright remedies that can be awarded against carriage service providers (the Part V, Division 2AA safe-harbour regime, from section 116AA on and in particular sections 116AG and 116AH).

The 'mere use of facilities' exception appears to have been intended to deal with situations where, for example, a company's liability might be said to arise only from ownership or control of telecommunication facilities used by a customer to infringe third-party copyright by communicating that subject matter. It is not clear that a user generated content internet content host "provides facilities for making, or facilitating the making of, a communication", or as to the circumstances in which less than actual knowledge of copyright infringement might suffice to make an internet content host more than a "mere" provider. As contended by David Brennan[44] in relation to the Sharman (**Kazaa**)[45] and Cooper[46] decisions:

> Coming through both cases was an acceptance that the post-Moorhouse case law establishes a broad concept of what can amount to authorisation. While a high level control coupled with indifference or wilful blindness might comprise authorisation (such as in Moorhouse itself), in other cases (such as in Cooper and Sharman (Kazaa)) marginal control would suffice if coupled with active encouragement. In the Full Court's consideration of Cooper, Branson J considered that arming or facilitation conduct alone could comprise the relevant control: 'a person's power to prevent the doing of an act comprised in a copyright includes the person's power not to facilitate the doing of that act by, for example, making available to the public a technical capacity calculated to lead to the doing of that act.[47]

The iiNet decision involved an ISP and users of that ISP accessing third party peer to peer sites. iiNet sold internet access to its subscribers in volumes measured by gigabytes. The terms of that service provision conferred upon iiNet power to cancel a service for illegal or unusual use. iiNet was alleged to have been uncooperative in working with the applicant copyright owners, represented by AFACT, to curtail the activities of persons engaging in unauthorised BitTorrent distribution of the applicants' copyright material using iiNet subscriber accounts. Had iiNet authorised infringements which occurred using accounts after iiNet had received AFACT notices which enabled iiNet to identifying those accounts?

Mr Justice Cowdroy's decision was 'no'. This answer was arrived at without recourse to the codified factors in determining 'authorisation' liability, as introduced by the 2001 amendments. Instead, the following passage from the judgement of Gibbs J in Moorhouse was particularly relied upon by Mr Justice Cowdroy:

> It seems to me to follow from these statements of principle that a person who has under his control the means by which an infringement may be committed – such as a photocopying

---

42 Copyright Act 1968 (Cth), sections 39B and 112E.

43 Copyright Act 1968 (Cth), section 116AH (1), Item 1.

44 Brennan, op cit at p 5.

45 Universal Music Australia Pty Ltd v Sharman License Holdings Ltd [2005] FCA 1242 (Wilcox J).

46 ibid; Universal Music Australia Pty Ltd v Cooper [2005] FCA 972 (Tamberlin J); Cooper v Universal Music Australia Pty Ltd [2006] FCAFC 187.

47 Cooper v Universal Music Australia Pty Ltd [2006] FCAFC 187.

machine – and who makes it available to other persons knowing, or having reason to suspect, that it is likely to be used for the purpose of committing an infringement, and omitting to take reasonable steps to limit its use to legitimate purposes, would authorize any infringement which resulted from its use.

Mr Justice Cowdroy reasoned that there could be no act of authorisation unless iiNet actually provided the 'means' of infringement. The broadband internet access supplied by iiNet was merely a "precondition to infringement", and not the "means". The "means" was found to be the BitTorrent protocol itself.

Upon finding no authorisation for failure by iiNet to supply 'the actual means of infringement', Mr Justice Cowdroy's consideration of the three mandatory factors in determining authorisation introduced by the 2001 amendments was obiter. The judge effectively considered together the first and third factors to find that the only judicially recognisable power to prevent was a power that was reasonable to exercise in all the circumstances. The court found that knowledge of infringement, even if coupled with the power to prevent such infringement, "is not, ipso facto, authorisation", in view of its earlier analysis. The applicants' case on authorisation had been that any ISP has a power to prevent infringing use undertaken using one of its subscriber's account and that this power converts to authorisation of that use at least at the point at which an ISP, having been given specific notice of ongoing infringing use, elects to take no action. A counter-view is that such notice may be specific as to past infringing use, but provide no reliable guide as to possible specific future acts of infringement. In any event, the decisions in Kazaa and Cooper had established that actual knowledge or encouragement of the primary infringement took a defendant outside the protection of the provision, because knowledge or encouragement meant that the authorisation arose from more than the 'mere use of the facilities' that had been provided by the defendant.

As noted in the preceding part of this paper, as at the date of this paper it was not clear whether the Gillard Government was waiting upon the appeal judgement of the Full Federal Court before further considering internet intermediary liability. Clearly the first instance judgement gives significant support to ISPs in an argument that they should not be required to intervene in respect of use by their users of third party peer to peer sites, and runs counter to 'graduated response' proposals. However, it is clear that significant concerns for copyright owners, ISPs and internet content hosts are raised from the reasoning in the judgement as that reasoning may be applied outside the third party peer to peer context. None of these players can be satisfied that in its current state, Australian copyright law is clear or predictable in its application to internet intermediaries.

The Australian safe harbours: Schedule 5 – Online Services to the Broadcasting Services Act

Schedule 5 – Online Services to the Broadcasting Services Act 1992 (Cth), as inserted by the Broadcasting Services Amendment (Online Services) Act 1999 (Cth) has a relatively short but controversial history.

The Schedule 5 framework was explained by the then Minister, Senator the Hon Richard Alston, as based upon the following considerations:

- the need for a uniform national framework to avoid "regulatory fragmentation" which would be the possible consequence of varying state and territory laws;
- the need for uniformity of content control as between the internet and conventional media;
- the need for recognition of the specific characteristics of the internet in considering the responsibility and potential liability of various players involved in the provision of internet-based content;
- the need to "meet the legitimate concerns and interests of the community while ensuring that industry development and competitiveness are not stifled by over-zealous laws, or inconsistent or unpredictable regimes";
- the recognition that user education (focusing in particular on the involvement of families) is critical in the adequate regulation of internet-based content.[48]

The relevant clauses read as follows:

> 90 Concurrent operation of State and Territory laws
>
> It is the intention of the Parliament that this Schedule is not to apply to the exclusion of a law of a State or Territory to the extent to which that law is capable of operating concurrently with this Schedule.
>
> 91 Liability of internet content hosts and internet service providers under State and Territory laws etc.
>
> (1) A law of a State or Territory, or a rule of common law or equity, has no effect to the extent to which it:
>
> (a) subjects, or would have the effect (whether direct or indirect) of subjecting, an internet content host to liability (whether criminal or civil) in respect of hosting particular internet content in a case where the host was not aware of the nature of the internet content; or
>
> (b) requires, or would have the effect (whether direct or indirect) of requiring, an internet content host to monitor, make inquiries about, or keep records of, internet content hosted by the host; or
>
> (c) subjects, or would have the effect (whether direct or indirect) of subjecting, an internet service provider to liability (whether criminal or civil) in respect of carrying particular internet content in a case where the service provider was not aware of the nature of the internet content; or
>
> (d) requires, or would have the effect (whether direct or indirect) of requiring, an internet service provider to monitor, make inquiries about, or keep records of, internet content carried by the provider.

Relevant definitions include:

> ***internet content*** means information that:
>
> (a) is kept on a data storage device; and
>
> (b) is accessed, or available for access, using an internet carriage service;
>
> but does not include:
>
> (c) ordinary electronic mail; or
>
> (d) information that is transmitted in the form of a broadcasting service.
>
> ***internet content*** host means a person who hosts internet content in Australia, or who proposes to host internet content in Australia.
>
> **internet carriage service** means a listed carriage service that enables end-users to access the internet.
>
> For the purposes of this Schedule, if a person supplies, or proposes to supply, an internet carriage service to the public, the person is an internet service provider.

48 Ibid at [90,000]; Senator the Hon Richard Alston, The Government's Regulatory Framework for Internet Content, (2000) 23 UNSWLJ 192 at p193.

The Government in its Explanatory Memorandum characterised its policy approach as follows:

- the framework in the BSA would not hold online service providers responsible for the content accessed through their service where the online service provider is not responsible for the creation of that content; however, online service provider rules in the BSA will require that an online service provider will not knowingly allow a person to use an online service to publish material that is or would be Refused Classification under National Classification Board guidelines or publication of which would otherwise be illegal under an applicable State or Territory law;
- the Attorney-General would encourage the co-operative development of uniform State and Territory offence provisions regulating online content users, including the publication and transmission of certain material by users; these provision will not regulate online service providers, except to the extent that an online service provider acts as a content originator.. .

the definition of 'internet content host' as a "person who hosts internet content in Australia" is particularly unhelpful

The (Revised) Explanatory Memorandum noted in respect of the safe harbour:

> Clause 91, in conjunction with clause 90, is intended to give practical effect to the principle that, in general, the Commonwealth will provide a nationally consistent framework for the regulation of the activities of Internet service providers and Internet content hosts, while the States and Territories will continue to carry primary responsibility for regulating content providers and users.

In subsequent practice the Federal Parliament has eschewed this demarcation in at least two ways:

- the stated role of the States and Territories as carrying "primary responsibility for regulating content providers and users' has been steadily eroded through Federal legislative activity, including the restricted access system content regime introduced as Schedule 7 of the Broadcasting Services Act 1992 (Cth) in 2007 and privacy and cybercrimes legislation;
- internet content hosts have not been subject to "a nationally consistent framework for … regulation".

More problematically, clauses 90 and 91 have a number of significant drafting deficiencies:

- The protections only apply with respect to "internet content". This does not include "ordinary electronic email" or material "transmitted in the form of a broadcasting service".
- An entity must fall within the specific definitions of "internet service provider", which clearly is limited to those that provide internet carriage services (which presumably may be either access or backbone services), or an internet content host. But the definition of 'internet content host' as a "person who hosts internet content in Australia" is particularly unhelpful. The author of this paper suggests that in the context of these provisions, 'host' should be taken to refer to the housing or storing of any internet content for or on behalf of any third party, therefore potentially including services that host all forms of user generated content, including user contributions to social networking sites, to the extent that such content is hosted, and regardless of the extent to which the service is also (or even primarily or predominantly) a service making available content originated by the owner of that site. Given the importance of the concept of 'internet content host' in determining whether particular categories of internet intermediaries are entitled to the protection of these provisions, it would be desirable for the categories of internet intermediaries that are to be regarded as internet content hosts to be much more clearly stated. It is unfortunate in this regard that clause 91 focuses on an activity – "hosting" – rather than the originator of content that is "hosted": this creates unnecessary confusion as to indirect or secondary infringement.
- It seems likely that the exclusion of liability "in respect of hosting" would also cover acts ancillary to the hosting function. For example, to the extent that liability might have been imposed for the provision of access to the hosted material (rather than simply its storage), it would be logical that the internet content host should obtain the benefit of the protection. However, the clause does not put this view beyond argument.
- Although the wording of the provisions seems to be sufficiently broad to cover any liability under State and Territory law, the provisions appear in a Schedule directed at regulation of objectionable content in a censorship sense, applying the cooperative national classification regime. There was no discussion or debate as to the operation of clause 91 in relation to other laws, including defamation, contempt, restrictions on court reporting, the law of torts, State criminal law or so on. This leaves some residual doubt as to how a court might construe the breadth of the safe harbour.
- Federal (Commonwealth) law is unaffected, yet many Commonwealth statures are silent as to the internet and difficult to apply to internet services. The provision is drafted as though the Commonwealth had undertaken a comprehensive review and overhaul of Commonwealth statutes to ensure their consistent application. In fact, the Commonwealth looked only at the regulation of objectionable content in a censorship sense in the drafting of Schedule 5. This creates two difficulties. Firstly, it reinforces the argument (referred to above) that clause 91 was not intended to operate in relation to other laws, including defamation, contempt, restrictions on court reporting, the law of torts, State criminal law or so on. Second, the provision is susceptible to being overridden by subsequent inconsistent Commonwealth statutory provisions which may have been drafted without adequately taking into account internet-based services. This problem is becoming more pressing as the Federal Government moves into new legislative areas with significant impact upon internet-based services, such as expansion of privacy law, whistleblower protection statutes, freedom of information, interception, data retention and cybercrime legislation.
- Clause 91 leaves internet intermediaries without any form of statutory protection in relation to filtering or monitoring activities, which might give rise to "awareness" as to the existence, if not the legality, of particular content. By contrast, section 230 of the Communications Decency Act expressly protects internet intermediaries in relation to filtering activities.
- The distinction between State and Territory and Federal legislation is increasingly difficult to apply in the context of to cooperative statutory schemes which depends upon inter-locking Commonwealth and State and Territory legislation such as the new Australian Consumer Law or even the National Classification Scheme itself. In this regard the statement in clause 90 that "it is the intention of the Parliament that this Schedule is not to apply to the exclusion of a law of a State or Territory to the extent to which that law is capable of operating concurrently with this Schedule" is likely to reinforce any argument that an internet content host is not entitled to protection from the operation of a subsequently enacted cooperative Federal scheme such as the Australian Consumer Law: an outcome

that may not have even been contemplated by the drafters of the Australian Consumer Law.

Of course, a key element in the analysis of the clause 91 exception is the requirement that the host (or ISP) was not aware of the nature of the internet content. So stated in the negative, in the context of clause 91 this should preclude any argument as to imputed or constructive knowledge, for example, that a user generated content site was commonly being used for uploading and downloading of actionable material. However, and as already noted, the term "awareness" does not have a body of judicial interpretation, unlike the concept of "knowledge" as extensively analysed in many statutory and common law causes of action. Clearly the Australian safe harbour falls away once an internet intermediary becomes aware as to "particular internet content": without doubt "aware" as to the existence of particular content but not necessarily "aware" that the content is infringing, leaving difficult questions as to when and how an internet content host or an internet service provider should take steps to determine whether content is infringing. Adrian Lawrence argues in the context of application of the provision to defamation law:

> ... this element of the provision could support a number of different interpretations. At its weakest, the provision could effectively remove the protection in circumstances where the host or service provider knew that the type of material was such that it could give rise to a liability in defamation. At its strongest, the provision could be interpreted to require actual knowledge that the particular material was defamatory. The correct position is no doubt somewhere between these two extremes, but its precise determination is problematic. A possible interpretation of the provision is that the host or service provider loses the benefit of the defence when the existence of the particular material is drawn to its attention. It is at that point that it must make a determination as to whether the material is in fact defamatory, and therefore whether to remove it from its network, or retain it and face the potential consequences of such an action. However, it is relatively clear that actual knowledge is required, as opposed to constructive knowledge.[49]

It is undesirable that clause 91 leaves such a degree of uncertainty as to the circumstances in which an internet content host is "aware" that actionable material is available on a service hosted by the service provider and that the material is properly to be considered illegal, as distinct from alleged by someone to be actionable. An internet content host may be made "aware" that material is available on a service hosted by the service provider, but unable reasonably to determine whether it is actionable or not: for example, it will often be impossible to determine from a complaint whether material alleged to be in breach of personal privacy is in fact in breach of a particular individual's personal privacy. Uncertainties as to the scope of operation of clause 91 may rightly be considered to have a chilling effect upon the development of user generated content and social networking sites hosted in Australia.

Conclusion

The Australian safe harbour provisions are relatively young in statute law terms. However, the internet, the rapid and unexpected evolution of user generated content sites and Web 2.0 applications such as mash-ups, blogging and social networking, requires the law to again adapt and evolve.

Web 2.0 applications facilitate complex inter-relationships between persons responsible for creation of particular (and often merged content) and the providers of the places where that content may be uploaded and viewed. The legal treatment of these complex inter-relationships requires finding answers to difficult questions of primary and secondary liability: in particular, as to the circumstances in which an internet intermediary should be treated as responsible in relation to wrongful acts by internet users. The solution in most jurisdictions has been to build limited 'safe harbours' for internet intermediaries, excepting an internet intermediary from liability in relation to wrongful acts by internet users so long as the intermediary complies with conditions attaching to the safe harbour.

European and United States 'safe harbours' have been built upon distinctions between 'information conduits' and content originators. These distinctions have only partially been imported into Australian law. Aside from the Copyright Act safe harbours, the only Australian statutory provision to afford a broader 'safe harbour', clause 91 in Schedule 5 of the Broadcasting Services Act 1992 (Cth), is uncertain as to scope and difficult to apply with any certainty. Federal statutes sit outside the Schedule 5 safe harbour, but there does not appear to have been systematic consideration of the operation of Federal statutes in relation to internet based services.

In the absence of any more general approach to safe harbours, development of the law in Australia will remain fragmentary, inconsistent and driven at different rates according to the politico-economic bargaining power of particular industry players and sectors. Laws developed to cater for traditional media and modes for distribution of copyright works are already being applied to Web 2.0 applications using outdated analogies and examples. At a time when the Federal Parliament endeavours to address media and communications convergence through new legislation, it is appropriate to also seek a converged approach to liability of internet intermediaries.

Peter Leonard heads the Communications, Internet and Media Team at Gilbert + Tobin Lawyers, where he has been a partner since 1989. The views expressed in this paper are the personal views of the author and not the views of Gilbert + Tobin Lawyers or its clients. This is an edited version of a paper delivered at the Communications and Policy Resaerch Forum 2010. A full version including all footnotes is available from the author upon request.

49 Op cit, "Defamation" chapter, para [70,270].