BUILDING SAFE HARBOURS IN CHOPPY WATERS — TOWARDS A SENSIBLE APPROACH TO LIABILITY OF INTERNET INTERMEDIARIES IN AUSTRALIA

PETER LEONARD
Partner, Gilbert + Tobin Lawyers

Summary

Many of the key principles of the common law and of intellectual property law were developed before widespread use of the internet. Many State and Territory statutes were drafted without clear territorial nexus provisions, on the reasonable view (before the internet) that it would be self evident when a particular activity took place within a particular State or Territory and who committed that act. The internet challenged many of these principles. Even in those few areas where the law was re-written or judge made law evolved to address 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 interrelationships 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 interrelationships 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 a few areas of Australian law. There is no unifying reasoning in Australian jurisprudence to promote and guide consistency across the various areas of law involved. The only Australian statutory provision to afford a broader ‘safe harbour’ lies unsung and little analysed in Schedule 5 of the Broadcasting Services Act. By contrast, broad form safe harbours in the European Union and the USA were developed after significant policy discussion and have then been extensively analysed and litigated.

In the absence of any unifying 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. This paper analyses the business and social policy underpinnings of safe harbours in law, the appropriateness of broad form protections, and the vexed distinctions between copyright and other areas of law.

---

1 Peter Leonard is a Partner of Gilbert + Tobin Lawyers. The views expressed in this paper are the personal views of the author and not the views of Gilbert + Tobin Lawyers or its clients.
Introduction

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 (ISPs), 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.2 That debate was further fuelled by criticisms as to secondary liability provisions of negotiating drafts of the proposed multilateral Anti-Counterfeiting Trade Agreement, styled by one critic as ‘the entertainment industry’s efforts to impose U.S. style DMCA copyright law on the globe’.3

There have also been detailed commentaries as to the operation of content laws in relation to Australian internet access service providers4 and the Federal Government’s proposal for mandatory provider side internet filtering.5

1 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 study6 in Australia: the operation of the limited safe harbour in 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:

---


4 See for example the ‘Censorship’ chapter in Adrian Lawrence The Law of Ecommerce, LexisNexis loose-leaf service, ongoing. A useful online resource on censorship in Australia with many links to other relevant material is the site maintained by Irene Graham at http://libertus.net/.


(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.7

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 limited and generally as incidental coverage as part of 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 most directly comparable provision under U.S. Federal law, section 230 of the Communications Decency Act of 1996,8 has been considered in numerous judicial decisions9 and academic treatise.10 The comparable provisions at the European Union level, Articles 14 and 15 of the Directive on electronic commerce (2000/31/EC)11 has been the subject of much less extensive

---


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

9 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.


academic treatment\textsuperscript{12} 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. The policy approach of section 230 and the EU Directive Articles 14 and 15 is markedly divergent in relation to the requirements imposed upon an internet intermediary when fixed with knowledge as to infringing content published by another person. The policy approach of section 230 is also markedly divergent from the ‘notice and take-down’ procedure in respect of copyright material pursuant to the U.S. Federal Digital Millennium Copyright Act\textsuperscript{13} (‘DMCA’) of 1998 and comparable provisions under Australian copyright law.\textsuperscript{14} The divergence of internet content law and copyright law as it applies to intermediaries also appears to be increasing as European States consider imposition of ‘graduated response’ requirements on internet intermediaries.\textsuperscript{15} Clause 91 sits uncomfortably within these divergent approaches, without any expressed policy rationale for its limited scope of coverage or different approach to that adopted under Australian copyright law.

Second, 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.\textsuperscript{16}

Third, for the reasons discussed later in this paper clause 91 is remarkably limited in its scope of coverage as compared to analogous U.S. and E.U. provisions (section 230 of the Communications Decency Act and Articles 14 and 15 of the EU Directive).

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.

The limited scope of coverage of clause 91 is best illustrated by comparison with section 230 of the Communications Decency Act and Articles 14 and 15 of the EU Directive. But it is first necessary to map out the battlefield.

2 Ruminations about intermediaries: impermissible or just plain impossible?

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 calibrated their language to ensure that they are arguing the same point. Let us first be clear as to the internet intermediaries under review, and the differences in exculpatory approaches and rules in major countries.


\textsuperscript{13} ss 201-203, codified as 17 USC §511-513.

\textsuperscript{14} Discussed below in Part 8 of this paper.


\textsuperscript{16} One of the few other Federal statutes broadly covering the internet is the \textit{Internet Gambling Act 2001}.
Internet intermediaries may be relevantly characterised in three groups:17

(1) communication conduits;
(2) content hosts;
(3) 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 (providing 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.

The second category of intermediaries comprises 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 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 unmodulated 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.18 The quantity of Facebook material is best illustrated by reference to user face time: in August 2010 it was estimated that over 10 per cent of total time online of US users was spent on Facebook as compared to 9.6 per cent on the Google family of services (Google Search, Gmail, YouTube, Google News, Google Earth and so on).19

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


Eric Sinrod, Face Time: Internet Users Stay on Facebook the Longest, 12 October 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.
facilitate patently illegal activity, including pirates being pirated: for example, a search query of ‘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 this consensual 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 liability20 and so much of the legislative agenda?21

---


21 Examples include the contentious multilateral negotiations as to the Anti-Counterfeiting Trade Agreement, well tacked in Michael Geist’s blog at www.michaelgeist.ca; the Canadian Copyright Modernization Act (Bill C-32) introduced 2 June 2010: an Act to amend the Copyright Act, http://www2.parl.gc.ca/HousePublications/Publication.aspx?Docid=4580265 summarised in Michael Geist’s blog at
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.\(^\text{22}\) Ms Reding observed:

> These figures reveal the serious deficiencies of the present system. It is necessary to penalise those who are breaking the law. But are there really enough attractive and consumer-friendly legal offers on the market? Does our present legal system for Intellectual Property Rights really live up to the expectations of the internet generation? Have we considered all alternative options to repression? Have we really looked at the issue through the eyes of a 16 year old? Or only from the perspective of law professors who grew up in the Gutenberg Age? In my view, growing internet piracy is a vote of no-confidence in existing business models and legal solutions. It should be a wake-up call for policy-makers.\(^\text{23}\)


\(^{23}\) Ibid.
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 audiovisual works, such as television shows and Hollywood movies, on BitTorrent and other peer to peer networks.\(^{24}\)

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 ISPs as the principal defendants in infringement proceedings.

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 poses particular challenges for copyright law in many countries as even recently developed statutory schemes did not anticipate user generated content. In some cases (e.g. Australia)\(^{25}\) these statutory copyright exemptions did not deal at all with copyright liability of content hosts. In other cases (e.g. many European countries, in their implementation of the eCommerce Directive)\(^{26}\) did not deal in sufficient clarity with the liability of content host intermediaries (as distinct from internet access and internet carriage intermediaries).

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 authorisation liability with 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 an intentional inducement or encouragement of the direct infringement; vicarious infringement requires profit from direct infringement where a right is held and not exercised to stop or limit that direct infringement.

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

\(^{24}\) IFPI Report, *op cit*.

\(^{25}\) Part V, Division 2AA, as inserted in the *Copyright Act 1968* (Cth) with effect from 1 January 2005, did not the test for authorisation of copyright infringement under section 36 and section 101 of the Copyright Act. Accordingly, an internet intermediary must be found to have authorised infringement of copyright before it needs to rely on the safe harbour provisions. An intermediary is not liable where they are ‘merely’ providing ‘facilities’ that a person uses to infringe copyright. In assessing authorisation liability by an internet intermediary, the Australian courts must consider the various factors outlined in s36(1A) and s101(1A), which include whether any relevant industry code has been complied with. However, the safe harbours in Part V, Division 2AA are expressly only available to ‘carriage service providers’, which would not include the many internet content hosting services which do include any carriage (communication) service component.

\(^{26}\) See Part 6 of this paper.
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.

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’ famously applied by the High Court of Australia in the Gutnick 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. 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 qualified by requirement of proof as to ‘actual knowledge’ as to the material being ‘wrongful’, or other limiting (or in some cases, exonerating) factors.


30 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
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.

In the U.S.A., various common law and statutory protections from secondary liability under various causes of action create what could best be described as a patchwork quilt of liability. In some respects the patchwork quilt is less daunting to anise than many other jurisdictions, because the two largest patches, being section 230 of the Communications Decency Act and the DMCA notice and take-down copyright provisions, occupy so much of the surface area of the quilt. But the other parches remain important and some remain subject to common law development.

Secondary liability has no direct equivalent under Anglo-Australian common law, although principles as to indirect infringement and authorisation (‘sanctioning, approving or countenancing’) are analogous. Much confusion arise from attempts to apply United States concepts of secondary liability to Australian causes of action, and this confusion is compounded by two factors. First, many of the causes of action are deceptively similar under Australian and U.S. jurisprudence, while the exoneration principles or defences are quite different. Second, many of the decisions in internet publication are made in California by application of principles of U.S. Federal or State law or projection as to what the 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.

### 3 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. Typically the safe harbours are piecemeal exceptions rather than broadly based exonerations and were carved out for particular intermediary activities, such as internet access services or provision of search engines, or in respect of particular causes of action, such as secondary (or indirect or authorisation) liability for infringement of copyright or liability in relation to offensive content. Each safe harbour is an attempt to effect a balance between the protection of rights holders and intermediaries’ right to develop technologies and business models that facilitate and enable reproduction and dissemination of digital information. In all cases these safe harbours have drafting deficiencies. These drafting deficiencies typically arise in one or both of two ways. First, each safe harbour was generally the output of a political compromise effected after heavy lobbying between rights holders and the internet industry. Sometimes the deficiency reflects a political compromise that is reflected in vague or open 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 -- or that the defendant would have been found liable under U.S. laws anyway. 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. David Johnson notes that ‘This could prevent enforcement in the U.S. of defamation suits regarding publications that were not expressly aimed at the jurisdiction in which the suit was brought — i.e. true libel tourism’: See *Epstein Becker Green Internet and E-commerce Law Blog*, 20 September 2010, at [http://www.internetecommercelaw.com/2010/09/articles/communications-decency-act/new-speech-act-provides-limited-protections-for-website-operators-authors-and-publishers-against-libel-tourism](http://www.internetecommercelaw.com/2010/09/articles/communications-decency-act/new-speech-act-provides-limited-protections-for-website-operators-authors-and-publishers-against-libel-tourism).
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.\(^{31}\)

An example of a broadly based safe harbour is section 26 of the Electronic Transactions Act 2010 of Singapore,\(^ {32}\) 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:

(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.

---

\(^{31}\) Division 2AA of the *Copyright Act 1968* (Cth) (Act), 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. The remedies available against online service providers are limited if they have complied with the conditions as contained in Division 2AA of the Act. For a brief outline of the legislative history of copyright safe harbours in Australia, see Melissa de Zwart, *The Safe Harbour UGC Business Model: judicial endorsement in Viacom v YouTube*, The Fortnightly Review of IP and Media Law, 15 July 2010 at [http://fortnightlyreview.info/2010/07/15/in-this-edition-11/](http://fortnightlyreview.info/2010/07/15/in-this-edition-11/).

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 did not include the copyright exception: this was later introduced following representations by rights holders and Singapore entering into the Singapore–USA Free Trade Agreement. The copyright safe harbour now appears as sections 193B to 193D and 252A to 252C of the Copyright Act (chap. 63) of Singapore, and broadly reflects the U.S. DMCA approach. 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 the curiously named Communications Decency Act, and 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.

4 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.

The provisions have a curious legislative history. Although section 230 is now seen as an important tool in the armoury of First Amendment protection of free speech, the provision is a remnant of an Act that was largely struck down by the U.S. Supreme Court as contrary to the First Amendment. That struck-down Act was introduced to enlist online service providers in the battle against indecency and to protect them from liability when they did so. The First Amendment rationale for giving broad operation to section 230 has now almost completely overshadowed the origins of section 230 and First Amendment driven court rulings have expanded the protection of section 230, including in respect of indecent material.

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. While some internet intermediaries may be willing to bear the cost

33 Effective 1 January 2004 and available at http://tcc.export.gov/Trade_Agreements/All_Trade_Agreements/exp_007049.asp.
34 See http://statutes.agc.gov.sg/.
36 Section 230(c) is headed ‘Protection for ‘Good Samaritan blocking and screening of offensive material’ and protects a provider or user of an interactive computer service from voluntary action to block availability of objectionable content. See the discussion in David Ardia, op cit pp. 409–12.
of staff and resources to manually review content, many will be unable or unwilling to do so, either because the volume of material makes manual checking impossible or because even a manual check would not enable a judgement to be made or because of economics. 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.

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’.37

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’.38

‘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 …’.39 The most common interactive computer services are, of course, websites.

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’.40 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.41 Taking an active role in editing content,42 and encouraging or soliciting others to submit content — including content that is likely to be actionable43 — has not disentitled defendants to section 230 immunity.

37 Ibid.
38 47 U.S.C. § 230(c)(1)
41 See Batzel v. Smith 333 F.3d 1018, 1031 (9th Cir. 2003) and decisions there cited.
Section 230 immunity is not lost once the publisher is on notice of the allegedly defamatory content. 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, 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).

5 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. 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:

44 The seminal case establishing this proposition is Zeran v. America Online, Inc 129 F.3d 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.
45 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.
46 At 1107: ‘Barnes does not seek to hold Yahoo! liable as a publisher or speaker of third-party content, but rather as the counter-party to a contract, as a promissor who has breached.’ At 1108.
47 47 U.S.C. §§230(e)(1),(2),(3) and (4).
must not receive a financial benefit directly attributable to the infringing activity;\(^{50}\)

must not be aware of the presence of infringing material or know any facts or circumstances that would make infring ing material apparent, and

upon receiving notice from copyright owners or their agents, act expeditiously to remove the purported infringing material.

One intermediary that was found to receive a direct financial benefit from infringing activity was Napster.\(^{51}\) The Napster court held that copyrighted material on Napster’s system created a ‘draw’ for customers, which resulted in a direct financial benefit because Napster’s future revenue was directly dependent on increases in user-base.

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.\(^{52}\) 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 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

---

\(^{50}\) This exception only applies where the service provider has the right and ability to control the infringing activity. In the summary judgement of Stanton USDCJ in Viacom & ors v YouTube & ors, ibid. Judge Stanton concluded that the provider must know of a particular case of infringement before the provider can control it. At pp. 24–5: ‘There may be arguments whether revenues from advertising, applied equally to space regardless of whether its contents are or are not infringing, are ‘directly attributable to’ infringements, but in any event the provider must know of the particular case before he can control it.’


\(^{52}\) The DMCA is explicit: it shall not be construed to condition ‘safe harbor’ protection on ‘a service provider monitoring its service or affirmatively seeking facts indicating infringing activity’: at section 512(m)(1); see also Senate Report at 44, House Report at 53; summary judgement of Stanton USDCJ in Viacom & ors v YouTube & ors, 2010 WL 2532404 (SDNY 23 June 2010). For further discussion as to the application of the DMCA provisions to Web 2.0 services, see Brandon Brown, Fortifying the Safe Harbors: Reevaluating the DMCA in a Web 2.0 World, 23 Berkeley Tech. L.J. 437, 438 (2008), and for an interesting analysis of the summary judgement in Viacom v YouTube, see Charles Sims and Elizabeth Figueria, YouTube, Google Find Safe Harbor in New York Court, Communications Lawyer, September 2010, pp. 3–5.
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.53

6 EU Directive on Electronic Commerce

8 June 200054 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 service55 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.

53 Ibid. The decision considers the Grokster line of cases and in particular the applicability of decisions in relation to
to peer-to-peer software to YouTube’s business model, and concludes: ‘The Grokster model does not comport with that
of a service provider who furnishes a platform on which its users post and access all sorts of materials as they wish,
while the provider is unaware of its content, but identifies an agent to receive complaints of infringement, and
removes identified material when he learns it infringes. To such a provider, the DMCA gives a safe harbor, even if
otherwise he would be held as a contributory infringer under the general law. In this case, it is uncontroversied that
when YouTube was given the notices, it removed the material. It is thus protected ‘from liability for all monetary
relief for direct, vicarious and contributory infringement’ subject to the specific provisions of the DMCA’. See
further Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd. 545 US 913 (2005) and its progeny Arista Records
5578, 2009 US Dist. LEXIS 122661 (C.D. Cal. 21 December 2009), and Arista Records LLC v. Lime Group LLC,
No. 06 Civ.5936 (KMW), F. Supp. 2d 2010 WL 22 91485 (SDNY 25 May 2010).

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.

55 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. For present purposes, it appears likely that the definition includes
hosting information provided by a recipient of the service, and provision of an online information service. See the
discussion in Timothy Pinto, Niri Shan and ors., Liability of Online Publishers for User Generated Content:
A European Perspective Communication Lawyer April 2010, at p. 5.
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.

(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.
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.

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.

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.

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’. 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 (Bundesgerichtshof) 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.

---

56 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, pp. 35/115–60/115, available at http://ec.europa.eu/internal_market/e-commerce/directive_en.htm.

57 See cases cited in Broder Kleinschmidt, op cit (footnote 11), pp. 15–16.
By contrast, English courts have rejected attempts of trade mark holders to compel eBay to prevent infringements of their customers.\(^{58}\) 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.\(^{59}\)

On 20 September 2010, YouTube successfully fought off a copyright infringement claim in the Madrid Commercial Court from Spanish broadcaster, Telecinco. Telecinco alleged that YouTube was not protected by the safe harbour rules because YouTube was performing an editorial role over that content: some videos posted by users were presented on the site as ‘featured videos’, and Telecinco alleged that in selecting those videos, YouTube had exercised editorial discretion. However, the court held that ‘featured videos’ were selected according to their popularity amongst users, rather than on a subjective basis. The court also considered that YouTube’s notice and take-down procedure complied with the requirement to ‘expeditiously remove … or disable access’ to the infringing material.

By contrast, the Hamburg District Court ordered YouTube to pay damages and to take down from its site three music videos featuring the singer, Sarah Brightman. The Hamburg District Court appears\(^{60}\) to have ruled that YouTube had assumed a degree of control over user generated content on its site, and therefore had a duty to check that the content was not infringing: the fact that YouTube requires users to confirm that they had the right to upload the material appears to have not been regarded as sufficient.

The status of Articles 14 and 15 will be tested by two recent referrals to the 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.\(^{61}\) The ECJ will be required to balance the safe harbours against European privacy rights and a provision the Information Society Directive\(^{62}\) 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 (14 November 2010) the European Commission was engaged in a Public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on electronic commerce (2000/31/EC).\(^{63}\) The period for consultation closed on 5 November 2010. The terms of reference included: ‘The regulation of the exemptions of the liability of intermediaries (Section 4, Articles 12 to 15) with a view to ensuring, on the one hand, the provision of basic intermediary services guaranteeing the free movement of information on the network and, on the other, a legal framework enabling the development of the internet and electronic commerce’. The Commission also solicited input as to ‘The interpretation of the provisions concerning the liability of intermediary information society service providers’.

\(^{58}\) Ibid, pp. 16–17, see further L’Oreal v eBay [2009] EWHC 1094 (Ch) 375; http://www.bailii.org/ew/cases/EWHC/Ch/2009/1094.html.

\(^{59}\) Ibid, p. 17.

\(^{60}\) A brief court statement was issued on 3 September 2010. A full transcript of the judgement was not available to the author at the date of writing this paper (14 November 2010).

\(^{61}\) See further Laurent Masson, Brussels court refers two questions to the ECJ on injunctions against ISPs over illegal P2P file sharing, Bird & Bird Bulletin 5 October 2010, at http://www.twobirds.com/English/News/Articles/Pages/Brussels_court_refers_ECJ_injunctions_against_ISPs_050510.Aspx.


7 Repeat infringers and graduated response

The DMCA requires internet intermediaries to remove repeat infringers. The effectiveness of the DMCA requirement has been extensively debated across the globe, most recently in the ‘three strikes and you’re out’ or ‘graduated response’ controversy. As stated by Judge Stanton in his summary judgment in Viacom & ors v YouTube & ors:

YouTube has implemented a policy of terminating a user after warnings from You Tube (stimulated by its receipt of DMCA notices) that the user has uploaded infringing matter (a ‘three strikes’ repeat-infringer policy). That YouTube counts as only one strike against a user both (1) a single DMCA takedown notice identifying multiple videos uploaded by the user, and (2) multiple take-down notices identifying videos uploaded by the user received by YouTube within a two-hour period, does not mean that the policy was not ‘reasonably implemented’ as required by § 512 (i) (1) (A). In Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1105 (W. D. Wash. 2004), in evaluating whether Amazon complied with § 512(i), the Court stated that even DMCA-compliant notices ‘did not, in themselves, provide evidence of blatant copyright infringement’. In UMG Recordings, Inc. v. Veoh Networks, Inc., 665 F. Supp. 2d 1099, 1116, 1118 (C.D. Cal. 2009), the Court upheld Veoh’s policy of terminating users after a second warning, even if the first warning resulted from a take-down notice listing multiple infringements. It stated: ‘As the Corbis court noted, [t] he key term, ‘repeat infringer,’ is not defined. The fact that Congress chose not to adopt such specific provisions when defining a user policy indicates its intent to leave the policy requirements, and the subsequent obligations of the service providers, loosely defined.’ Corbis, 351 F.Supp.2d at 1100-01. This Court finds that Veoh’s policy satisfies Congress’s intent that ‘those who repeatedly or flagrantly abuse their access to the Internet through disrespect for the intellectual property rights of others should know that there is a realistic threat of losing that access’: H.R. Rep. 105-551(II), at 61.

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 currently less clear. There have also been very interesting decisions considering the proportionality of graduated response in the Irish High Court. Although each country has adopted or proposes different balances, the key characteristics of these systems 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.

---


65 See House of Commons of Canada, Bill C-32: An Act to amend the Copyright Act, as first read 2 June 2010, available with links to many commentaries through [http://www.michaelgeist.ca/](http://www.michaelgeist.ca/).


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.\textsuperscript{68}

Issues raised as to intervention of an internet access service 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. However, the above identified issues around graduated response proposals should have particular traction in jurisdictions where there is not a constitutionally guaranteed freedom of speech and communication, as the courts in such jurisdictions will have limited authority or basis to control over zealous expansions of graduated response. Some proposals for graduated response endeavour to address these issues: for example, the Canadian ‘notice notice’ proposal\textsuperscript{69} 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 \textit{Australian Digital Economy: Future Directions}\textsuperscript{70} 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.\textsuperscript{71} The final paper of July 2009 stated:

> The issue is that it is unclear whether the present scheme works effectively for some types of online service providers that have subsequently grown in popularity as new platforms for social engagement, content distribution and political communications since the scheme’s introduction. Uncertainty about whether newer digital economy platforms are covered by the safe harbour may interfere with the ability of providers of these platforms to effectively develop business models in Australia. Examples of some of the types of platforms that may not be carriage

---

\textsuperscript{68} 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 \url{http://www.europarl.europa.eu/oeil/file.jsp?id=5817632}; the Gallo Report is also available at that address.

\textsuperscript{69} House of Commons of Canada, \textit{Bill C-32: An Act to amend the Copyright Act}, as first read 2 June 2010; see further the discussion at Michael Geist’s blog, \url{http://www.michaelgeist.ca/}, and Barry Sookman’s blog, \url{http://www.barrysookman.com}.

\textsuperscript{70} Available at \url{http://www.dbcde.gov.au/digital_economy/future_directions_of_the_digital_economy/australias_digital_economy_future_directions}.

\textsuperscript{71} Submissions are available at \url{http://www.dbcde.gov.au/digital_economy/future_directions_of_the_digital_economy/submissions}. 
service providers and, consequently, may not come within the present scheme include social networking and user-generated content sites.

The consultation draft of this paper queried whether an examination of the scope of Australia’s safe harbour scheme would be beneficial, in particular whether its scope, consistent with international obligations under the AUSFTA, should be expanded to encompass a larger range of online services that are important to the digital economy. A number of submissions addressed this issue. Overall, slightly more submissions were in favour of an expansion of the present scheme. Of those who favoured expansion, reasons given included that the expansion would:

- remove a barrier to the next Flickr/Facebook/YouTube being developed in Australia (proponents noted that these sites had all developed in the US which enjoys a more expansive scheme)
- provide greater certainty to digital economy platforms and attract their investment into Australia
- increase the global competitiveness of Australia’s online businesses
- position Australia on par with leading trading partners in the Asia–Pacific region, thereby maintaining the attractiveness of Australia as a regional hub
- promote innovative and collaborative uses of technology that fulfil user demands and help Australia realise its potential to become a global centre for innovation.

Of those who opposed the expansion, the reasons given included that:

- the existing scheme had failed to encourage ISPs to cooperate with copyright owners and, consequently, it was not appropriate to broaden them
- digital economy platforms should be developed through licensing arrangements instead of safe harbours
- expansion would not harmonise Australia’s law with the US but would secure a windfall benefit without imposing the corresponding obligations on service providers to disclose details of alleged infringers
- there is a lack of evidence that the existing scheme discourages the proliferation of localised versions of these digital economy platforms in Australia
- the safe harbour scheme may be judicially considered in the current litigation between the Australian Federation Against Copyright Theft and iiNet.

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.

As at the date of this paper (14 November 2010) it was not clear whether the Gillard Government was waiting upon the outcome of the appeal to the Full Federal Court from the first instance decision of Mr Justice Cowdroy in the iiNet case, or delaying its response for other reasons. That noted, there were media reports to the following effect:

The federal Attorney-General, Robert McClelland, is in favour of a review of copyright by the Australian Law Reform Commission (ALRC), while the Greens have included copyright reform as a key element in their arts policy. In late September the Australian Financial Review quoted the Attorney-General as saying that Australia would benefit from an ALRC review of copyright legislation: ‘It is very complex. There are obviously competing interests between consumers, service providers and networks … I think the best way to approach it is with genuine expert advice.’ The Attorney-General’s office has since confirmed his interest in a review by the

---

73 Ibid, pp. 21–2. The iiNet decision is briefly discussed below in this paper, at Part 8.
74 As at 14 November 2010, fully heard and awaiting the judgement of the Full Federal Court.
ALRC, adding that cross-portfolio consultation and agreement on terms of reference would be required before the Government announced such a review.75

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

It is outside the scope of this paper to enter into a detailed examination of the safe harbours under the Australian Copyright Act 1968.76 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 14 November 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 Moorhouse77 (Moorhouse) which involved the provision of a form of services to the direct infringer. ‘Trap infringing copying’ was undertaken in a university library from a copy of book held in the library, on a coin-operated photocopier situated 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.78

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’.79 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

---

77 University of New South Wales v Moorhouse (1975) 133 CLR 1.
78 Copyright Act 1968 (Cth), sections 36(1A) and 101(1A).
79 Copyright Act 1968 (Cth), sections 39B and 112E.
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.80

In 2004, in fulfilment of obligations under the Australia–US Free Trade Agreement (AUSFTA),81 the Federal Government enacted a copyright safe-harbour regime modelled on US copyright law, now Part V, Division 2AA of the *Copyright Act 1968*. 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’.82

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

---

80 House of Representatives, Chamber Hansard, Copyright Amendment (Digital Agenda) Bill 1999 Second Reading Speech, Daryl Williams MP, 2 September 1999, 9750. See further the analysis of the authorisation cases in David Lindsay, *op cit.*: ‘While some control is always required, the question of the degree or nature of that control may vary according to the circumstances. 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) 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’.

81 AUSFTA article 17.11(29).

82 *Copyright Act 1968* (Cth), section 116AH (1), Item 1.
content host more than a ‘mere’ provider. As contended by David Brennan\textsuperscript{83} in relation to the \textit{Sharman (Kazaa)}\textsuperscript{84} and \textit{Cooper}\textsuperscript{85} 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 willful blindness might comprise authorisation (such as in Moorhouse itself), in other cases (such as in \textit{Cooper} and \textit{Sharman (Kazaa)}) marginal control would suffice if coupled with active encouragement. In the Full Court’s consideration of \textit{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.’\textsuperscript{86}

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 AFAC\textsuperscript{T}, 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 AFAC\textsuperscript{T} 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 \textit{Moorhouse} was particularly relied upon by Mr Justice Cowdroy:

\begin{quote}
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 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.
\end{quote}

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 \textit{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

\textsuperscript{83} Breenan, \textit{op cit} at p 5.
\textsuperscript{84} \textit{Universal Music Australia Pty Ltd v Sharman License Holdings Ltd} [2005] FCA 1242 (Wilcox J).
\textsuperscript{85} \textit{ibid}; \textit{Universal Music Australia Pty Ltd v Cooper} [2005] FCA 972 (Tamberlin J); \textit{Cooper v Universal Music Australia Pty Ltd} [2006] FCAFC 187.
\textsuperscript{86} \textit{Cooper v Universal Music Australia Pty Ltd} [2006] FCAFC 187.
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 (Part 7) of this paper, as at the date of this paper (14 November 2010) it was not clear whether the Gillard Government was waiting upon the appeal judgement of the Full Federal Court87 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.

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

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

Adrian Lawrence summaries the controversy on passage of the Bill well, as follows:

To say that the bill and subsequent Act were controversial and stimulated a range of responses is an understatement. At the time of its introduction, the regime was variously described by advocates and commentators alike, ranging from its proponents in government:

The proposed regulatory framework … strikes a balance between the needs and interests of the industry and wider community concerns in relation to material that is illegal or highly offensive, or may be harmful to children …

to supporters of the regime as an inevitable compromise in the face of an otherwise unregulated and technically overwhelming situation:

… overall, the Online Services Act is to be applauded. It represents a serious attempt to address the availability to children of material on the Internet that the Australian community has already decided should not be readily available to children. In our view, it is indisputable that the need for a sheriff at the frontier is at least as great as it is in the settled areas …

to those who view the legislation as misguided, having a negative effect on the internet industry in Australia, and potentially unworkable in fundamental ways:

Broadcasting Services Amendment (Online Services) Act 1999 (Cth) … confused, ill conceived and very difficult to implement in practice … The Internet industry is left pondering how much damage it will cause to Australia’s emerging ecommerce infrastructure.

Certainly, the introduction of the Act was characterised by an inordinate amount of political manoeuvring, not least due to the practical need of the government to attract the vote of the staunch anti-pornography independent Senator Brian Harradine for its goods and services tax

87 As at 14 November 2010, fully heard and awaiting the judgement of the Full Federal Court.
legislation, but also due to the highly emotive subject matter, involving an ‘ongoing battle between libertarianism and social conservatism’.  

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.

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.

---

88 Adrian Lawrence, *Law of Ecommerce*, op cit, ‘Censorship’ chapter at [90,000]. The *Communications Legislation Amendment (Content Services) Act 2007* (Cth) upon enactment of a new Schedule 7 of the *Broadcasting Services Act 1992* (Cth) largely removed internet content hosts from the provisions of Schedule 5. However, clauses 90 and 91 of Schedule 5 were not amended.

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.

The Government characterised its policy approach (so far as currently relevant) 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 (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 in 2007 and privacy and cybercrimes legislation;

- internet content hosts have not been subject to ‘a nationally consistent framework for … regulation’.

---

90 Schedule 5 — Online Services to the Broadcasting Services Act 1992, clauses 3 and 8(1).


92 Ibid, notes to clause 91.
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

---

93 The Explanatory Memorandum noted “The exclusion of “ordinary electronic mail” from the definition of Internet content is intended to make it clear that the exclusion only applies to what an ordinary user of the Internet would regard as being e-mail, and that the exclusion does not apply to other forms of postings of material, such as postings to newsgroups. The term is also intended to minimise the scope for technical arguments about the “outer boundaries” of the term “e-mail” within the Internet community. The definition of “ordinary electronic mail” makes it clear that the term will not include a posting to a newsgroup. These provisions are intended to ensure that personal e-mail is not caught by the definition of “Internet content”.”

94 Now problematic because many internet streaming audiovisual service may in fact fall between a ‘broadcasting service’ and an ‘internet carriage service’, creating potential exposure for providers of content hosting services. Section 6 of the BSA defines ‘broadcasting service’ broadly to mean a service that delivers television programs or radio programs to persons having equipment appropriate for receiving that service, whether the delivery uses the radiofrequency spectrum, cable, optical fibre, satellite or any other means or a combination of those means, but does not include [paragraph (b) of Section 6] a service that makes programs available on demand on a point-to-point basis, including a dial-up service. The Explanatory Memorandum to the BSA states that the exclusion in paragraph (b) of the definition of ‘broadcasting service’ encompasses those services which allow a person to receive or access a program at a time determined by the person making a request. That is, where the scheduling of the program is determined by the service provider, the service is not a ‘point-to-point’ service. However, a Ministerial Determination under paragraph (c) of the definition of ‘broadcasting service’ (No. 1 of 2000) dated 12 September 2000, Commonwealth of Australia Gazette No. GN 38, 27 September 2010, determines that ‘a service that makes available television programs or radio programs using the Internet’ is not a ‘broadcasting service’, adding further confusion.

95 Consider, for example, a newspaper website, where almost all content is originated from the newspaper (or its affiliates) but which includes discussion forums or other feedback or comment fields for users, posted without pre-moderation.
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 statutes 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.

- 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. 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.97

---

96 For a good description of this scheme, see the Attorney-General’s Department website at [http://www.ag.gov.au/www/agd/agd.nsf/Page/Classificationpolicy_Nationalclassificationscheme](http://www.ag.gov.au/www/agd/agd.nsf/Page/Classificationpolicy_Nationalclassificationscheme); or for a less reverent (but very good) analysis, Irene Graham’s blog at [http://libertus.net/censor/clscensor.html](http://libertus.net/censor/clscensor.html).

97 Op cit, ‘Defamation’ chapter, para [70,270].
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.

10 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 interrelationships 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 interrelationships 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, 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.