PIRACY, FILE SHARING … AND LEGAL FIG LEAVES [*]

John Lambrick
General Counsel, RMIT University
Melbourne, Australia
john.lambrick@rmit.edu.au

Abstract. Peer to Peer (P2P) platforms have been very effective in allowing the transmission of large, bandwidth-intensive files (such as music and video) over the internet. Many such platforms are open source, and have been established by various operators as systems for the unauthorised distribution of copyright protected content.In addition to civil (and often criminal) liability faced by persons establishing P2P platforms for the unlawful distribution of content, an end-user who downloads copyright protected content from an unauthorised site risks civil action by the copyright owner for breach of copyright by making an unauthorised copy of the file.The paper will look at the significant growth in P2P file sharing and its role as a medium for copyright piracy. The paper will examine: how P2P file sharing facilitates internet piracy; the effect of case law; legislative changes which have taken place in an attempt to deter illegal distribution of copyright material through P2P platforms.; the effectiveness of strategies adopted by rights holders in an attempt to reduce unauthorised file sharing and ; protection measures available both for copyright owners seeking to avoid having their work illegally copied , and also third parties (such as ISPs and content hosts) who may unknowingly become involved in the distribution of such material.

1. Introduction

Piracy has always been a source of aggravation for those holding rights in intellectual property, but grudgingly acknowledged by them as a consequence of doing business in that field. The emergence of the internet, where valuable digital products can be copied with ease and widely distributed, has created an increased threat to copyright owners and distributors.

Until recently, technical difficulties associated with transferring large files offered some protection against the piracy of music and video over the internet. However, the development of MP3 and other compression technologies has meant that rich and bandwidth intensive files are now more vulnerable to copyright breach and piracy over the internet. The International Federation of the Phonographic Industry ("IFPI") has estimated that almost 20 billion songs were illegally downloaded in 2005 [1] and Music Industry Piracy Investigations ("MIPI") has estimated that in Australia around 2.8 million people, or 18% of the population illegally download music through file sharing every year [2.]

In terms of motion picture films, the Motion Picture Association of America ("MPA") has estimated that through piracy its member companies lose in excess of $US 896 million in potential revenue annually in the Asia Pacific region alone3. Piracy of motion picture films has to a large extent been effected by the illegal burning of digital video disks, but applications which distribute both music and video through peer to peer file sharing have added a very effective string to the bow of the audio-visual pirate.

2. What is Peer to Peer (P2P) Computing?

P2P computing involves the sharing of resources between computers by direct exchange between those computers. Unlike traditional network architecture which is based around client and server, the P2P network relies on the processing power of its individual computers. There is no reliance upon a centralised server, and each user's computer effectively becomes a server. In terms of file sharing, P2P computing enables users to connect to the hard drives of other users and to share files[4].

Whilst P2P computing has gained notoriety for facilitating internet piracy, it does have legitimate uses. In fact, Ashwin Navin, the President and Chief Executive of BitTorrent Inc. which provides the BitTorrent delivery

---

[*] This article was originally published in Kierkegaard, S. (2008) Synergies and Conflicts in Cyberlaw. IAITL .pp.365-380

[1] IFPI Piracy Report 2006: www.ifpi.org (Accessed 28 July 2008)

[2] www.mipi.com.au/about_piracy/musicpiracy.htm (Accessed 28 July 2008)

[3] Media Release October 24, 2005: www.mpaa.org (Accessed 28 July 2008)

[4] See http://www.utexas.edu/its/secure/articles/peer-to-peer_perils.php (Accessed 29 July 2008)

platform, has expressed the view that P2P is fundamentally the only way to deliver content on the internet without breaking the internet itself![5] (The contrary assertion is that BitTorrrent hogs bandwidth, and at times accounts for fifty percent of internet data traffic[6]). In any event, legitimate uses of P2P computing include:

- *Data co-ordination*. P2P technology can be used by organisations to provide workers with data and co-ordinate activities on large projects where little infrastructure exists. For example, humanitarian groups operating in Iraq have used P2P technology to synchronise the distribution of aid.[7]
- *Lawful sharing of copyright and public domain material*. Through file sharing, P2P technology enables content publishers who wish to make significant content available to large numbers of people to distribute that content at minimal cost.[8]
- *Distributed computing*. P2P technology enables idle disk space and processing power to be utilised, meaning that organisations can create a virtual supercomputer by aggregating unused computing resources (eg. desktops).

Because online file sharing utilising P2P technology effectively involves participants providing open access to the contents of their hard drives, the technology is not without risk. These risks include[9]:

- *Breach of privacy/loss of personal information.* Many people store highly sensitive personal information (bank account details, financial statements etc.) which can become available to others who access their hard drive.
- *Spyware.* P2P applications can be used by hackers to install spyware on a person's computer. Spyware can monitor keystroke activity and therefore ascertain passwords.
- *Viruses.* Viruses are often spread through P2P applications.
- *Exposure to legal risk.* Injudicious use of P2P file sharing can result in users being subjected to legal action where their use involves the unauthorised downloading or distribution of copyright material, or the unintentional downloading of illegal material (eg. child pornography).

P2P file sharing technology has become the distribution mechanism of choice for the internet copyright pirate. This paper will examine why this has occurred, the legal implications for those involved, likely future trends, and recommendations for those involved in the distribution of copyright material over the internet.

3. Why does P2P File Sharing make Rights Holders Nervous?

P2P file sharing has created considerable nervousness amongst rights holders, as evidenced by the following statement by MIPI:

> "In the last few years, sites that facilitate P2P file sharing have proliferated on the internet, resulting in hundreds of millions of dollars in lost revenues to artists and rights holders around the globe. These P2P sites are depriving the recording artists, composers, authors and record companies of the right to choose the value of their creative property in a free and open market."[10]

The reasons for such nervousness are both technical and legal.

3.1. Technical Issues

3.1.1. A decentralised environment

The first significant P2P copyright breach case was the Napster case[11.] Napster utilised a web site and P2P file sharing software to facilitate the swapping of MP3 music files. Many of those files were not authorised for distribution. Importantly, the Napster site contained a central directory which informed users as to what music was available for download from other users, although the files themselves were not stored centrally by Napster. Napster was (on the basis of United States copyright law) found liable for contributory infringement and to be

[5] "The Age" (Melbourne, Australia) November 7, 2006: "Torrents of users town P2P leaders towards licences, sale"
[6] "An Exaflood of peer to peer video expected" The Australian, April 1, 2008.
[7] Alan Davidson Centre for Democracy & Technology: "Peer to Peer File Sharing, Privacy & Security": www.cdt.org/testimony/030515davidson.shtml (Accessed 29 July 2008)
[8] Ibid
[9] Op cit n. 4 above
[10] http://www.mipi.com.au/about_piracy/musicpiracy.htm
[11] A&M Records Inc. v Napster Inc. 114F. Supp. 2d 896 (N.A. Cal. 2000)

vicariously liable for direct breaches by its users. On general copyright principles, it was always going to be difficult for Napster to avoid accountability for copyright breaches by its users.

However, P2P platforms can and now do operate in a highly decentralised manner. Many post-Napster networks are not maintained by a central body. Rather, the platform establishes users as a network of nodes which interconnect with each other[12]. Whilst the lack of centralisation does not necessarily mean that those establishing a P2P platform can avoid accountability where users breach copyright (the Kazaa decision[13] illustrates this) the less centralised that a P2P platform may be, the more difficult it is for rights holders to close it down where copyright breaches are involved.

3.1.2. Ability to distribute very large files – BitTorrent

For a time, the impracticalities (mainly significant delay) associated with transferring very large files over the internet provided some protection to the motion picture industry against internet based copyright breach. That is no longer the case. The BitTorrent[14] P2P content delivery platform has become a highly efficient means of distributing very large files over the internet, and with high quality. Downloads using BitTorrent are rapid because the process involves the downloading of the file in small portions from a number of different computers until the entire file is obtained. The effect is that a number of BitTorrent users share the bandwidth burden required to download a file which may otherwise take a number of days to download using another P2P platform such as Kazaa[15].

BitTorrent involves the use of a "tracker" file which contains specifications of the file downloaded and a history of the users who have previously downloaded the file[16].

3.2. Legal Issues

3.2.1. Jurisdiction

To date, rights holders have been quite ready to take legal action against the creators or providers of the P2P platform[17] or against the individual file sharers themselves[18] for copyright breaches effected through P2P file sharing. But this is not without difficulty. Creators or providers of P2P platforms can establish those platforms in jurisdictions with comparatively less restrictive copyright laws than the jurisdiction of the rights holder[19]. The jurisdictional problem is well illustrated by the now defunct (but once popular) Russian file-sharing service, AllofMP3 which offered music downloads at prices which were significantly cheaper than those of mainstream services, such as iTunes. AllofMP3 claimed to operate in accordance with Russian law[20], but the United States intervened politically with threats made that Russia risked its World Trade Organisation membership unless AllofMP3 was closed down[21]. The Russian government succumbed to this pressure, and the site was closed down in mid 2007[22].

The individual file sharers are usually individuals scattered all over the world who are often impecunious. This, of course, also creates problems for enforcement of court judgments.

3.2.2. Proof of ownership

Enforcement problems can also arise with proof of ownership. Digitised material can be made available instantaneously across many jurisdictions, and it can often be difficult to prove that a defendant did not have the right to copy such material[23].

---

[12] Guy Douglas: Copyright and Peer to Peer Music File Sharing: The Napster Case and the Argument Against Legislative Reform. www.murdoch.edu.au/elaw/issues/v11n1/douglas111_text.html (Accessed 29 July 2008)
[13] Universal Music Holdings Australia Pty Ltd v Sharman License Holdings Ltd (2005) 220 ALRI.
[14] www.BitTorrent.com (Accessed 29 July 2008)
[15] See Juliana Torres "Program fools peer-to-peer pirates" 27 April 2005 http://media.www.dailytexanonline.com/media/storage/paper410/news/2005/04/27/Focus/Program.Fools.PeerToPeer.Pirates-941102.shtml (Accessed 29 July 2008)
[16] op.cit
[17] See for example, the Napster case (n 11 above) and Kazaa case (n 13 above)
[18] See for example, "File Sharers Facing Legal Action" BBC News: http://news.bbc.co.uk/2/hi/technology/6058912.stm (Accessed 29 July 2008)
[19] Seagrumn Smith: "From Napster to Kazaa: The Battle over Peer to Peer File Sharing Goes International" www.law.duke.edu/journals/dltr/articles/2003dltr0008.html (Accessed 29 July 2008)
[20] Discussed by Darren Meale and Joel Smith in "All you MP3 are belong to us: a Russian tale of copyright woes". World Copyright Law Report, March 15, 2007.
[21] Nate Anderson "US: AllofMP3.com at the top of notorious markets list", 5 October 2006, http://arstechnica.com/news.ars/post/20061005-7915.html (Accessed 29 July 2008)
[22] "Russia Shuts Down AllofMP3.com" Times Online, July 2, 2007
[23] Tony Frone, "High Tech Crime Brief" Australian Institute of Criminology: www.aic.gov.au/publications/htcb/htcb003.html (Accessed 29 July 2008)

4. Liability for Copyright Piracy through P2P File Sharing

On general copyright principles applicable in jurisdictions which have adopted the World International Property Organisation ("WIPO") Copyright Treaty, the mere use by a person of a P2P platform should not of itself constitute a breach of copyright, as in most cases such platforms are made freely available for use by file sharers[24]. Copyright liability issues arise where the P2P platform is used to transfer files containing copyright works without the permission of the copyright owner.It is appropriate to consider liability in the context of:

- the creators or operators of P2P platforms
- users (downloaders/uploaders)
- content hosts/carriers/ISPs (intermediaries).

I will consider the issue principally in reference to liability for breach of copyright under the Australian Copyright Act 1968, with some comparative analysis in respect of other jurisdictions.

4.1. Creators or operators of P2P platforms

The United States legal doctrines of contributory infringement and vicarious liability under which Napster was found to be liable do not apply in Australia[25]. Where P2P file sharers unlawfully share files containing copyright material, the creator or operator of the P2P platform can be liable under sections 36(1) and 101(1) of the Copyright Act 1968 for "authorising" a breach of copyright.
In the *Kazaa* case[26] the Australian Federal Court held that the operator of the Kazaa platform were liable for any authorising infringements by file sharers, partly because it had the capacity to implement filtering systems which would curtail the sharing of copyright protected music, but failed to do so[27].

It is apparent from the Kazaa decision that a bona fide operator of a P2P system may avoid liability for authorisation breach if it takes appropriate steps (such as file filtering) and otherwise acts to discourage the unlawful sharing of copyright protected material. This may also be the position in the United States after the Grokster decision[28.] Some commentators have expressed the view that the Grokster decision appears sufficiently narrow as to allow P2P file sharing platforms to operate as long as they do not actively induce copyright infringement[29]. In Grokster the United States Supreme Court recognised that P2P file sharing can occur lawfully, but found Grokster liable for breach of copyright under a new concept of "inducement".

4.2. Users (Downloaders/Uploaders)

The Copyright Act 1968 imposes strict liability. Whilst the state of mind of an infringing party is relevant to the question of damages, it is not relevant to establishing a breach of the copyright owner's exclusive rights.

Included in the bundle of exclusive rights held by the owner of copyright in a sound recording are the right to make a copy of the sound recording and the right to communicate the work to the public[30]. The exclusive rights held by the owner of copyright in a cinematograph film include the right to make a copy of the film and the right to communicate the film to the public[31.]

Typically, when a user downloads a file using a P2P platform, the P2P software will provide for the file to remain on the user's computer, available for download by other users. Where the user downloads copyright material without authorisation, he or she directly breaches the owner's exclusive right to make a copy of the work. But liability may not end there, as subsequent uploads from the user's computer (then acting as a server) will result in the user directly breaching the copyright owner's exclusive right to communicate the work to the public – perhaps many times.

---

[24] Australian Vice Chancellor's Committee: "Peer to Peer File Sharing: the Legal Landscape" November 2003 http://www.universitiesaustralia.edu.au/documents/publications/policy/statements/P2P_file_sharing.pdf (Accessed 29 July 2008)
[25] Guy Douglas, op cit 12 at page 8
[26] Op cit n 13
[27] See Michael Williams: "File Sharing in the brave new world: peer-to-peer after Kazaa begins filtering its files". Vol 9, Numbers 6 & 7 Internet Law Bulletin, p.83 (LexisNexis Butterworths)
[28] MGM Studios Inc. v Grokster Ltd 545 U.S. 913 (2005)
[29] Rick McDermott v Joe Bracken: "MGM v Grokster and what it means for the future of P2P file sharing". World Copyright Law Report, March 23, 2006
[30] Copyright Act 1968, Sec. 85
[31] Copyright Act 1968, Sec. 86

More generally, rights holders have had no doubts as to the issue of liability and the viability of legal action against users. As at July 2006, the Recording Industry Association of America ("RIAA") had over a period of three years sued over 20,000 users for the unauthorised sharing of music files[32].

4.3. Content Hosts/Carriers/ISPs (Intermediaries)

Under Australian copyright law, it is unlikely that a telecommunications carrier or an internet service provider ("ISP") would be directly liable for copyright piracy or other breaches effected by P2P platforms operating through their infrastructure, provided that they are not responsible for determining the content of the material in question[33].

Liability of content hosts, carriers, ISPs or other intermediaries for copyright piracy or other breaches effected through their infrastructure would more likely be determined on the basis of authorisation. In this regard, some comfort is given to them by the Act[34] which confirms that a person who provides facilities in respect of a communication is not taken to have authorised an infringement of copyright merely because another person uses those facilities to effect the infringement.

In determining whether there has been an infringement effected through authorisation, the Act sets out an inclusive list of factors to be taken into account by the Court[35]. These are:

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

To date, no industry code of practice has been adopted in Australia.

Even if an intermediary is found to have authorised a breach of copyright, its liability may be limited if it has complied with the "safe harbour" provisions implemented to harmonise United States and Australian copyright law pursuant to the Free Trade Agreement recently signed between those countries. As a result of legislation implementing that agreement[36] the Copyright Act contains a new Part V, Division 2AA which has "safe harbour" provisions and a take down procedure for carriage service providers. In order to benefit from the provisions all carriage service providers must have a policy of terminating the accounts of repeat infringers and must not interfere with any technological protection measures of the content owner. In addition, carriage service providers who merely provide transmission or routing services must not have initiated the transfer of the copyright material, which material must also be transferred without substantial modification. Content hosts are subject to additional requirements being that they must not receive a financial benefit from the infringing activity and must remove infringing material upon receipt of a take down notice[37]. Note that there is no express obligation to monitor use or filter content.

Provided that carriage service providers (including ISPs) comply with the new provisions, they will not be liable for damages – which could otherwise be substantial for commercial scale piracy. Liability would be confined to such matters injunctive relief, orders to terminate an account or to remove infringing content. A significant limitation to the legislation is that the "safe harbour" provisions apply only to a 'carriage service provider' as defined in the Australian Telecommunications Act 1997 and would not apply, for example, to a university unless the university was registered as a carriage service provider under that Act.

In the European Union, the liability of ISPs and other intermediaries is governed by the Electronic Commerce Directive[38]. Article 12 absolves service providers from liability provided that in providing their communication network they act as a "mere conduit" and Article 13 provides an exemption for caching for the purposes of transmission efficiency. Article 14 deals with the liability of service providers who act as contents hosts, providing that they will not be liable for posting information "provided they do not have actual knowledge that the activity is illegal, and, upon obtaining such knowledge, act quickly to remove or disable access to the relevant information". Article 15 provides that member states cannot impose a general obligation on service providers to monitor content.

4.4. Criminal liability

[32] "How Not To Get Sued for File Sharing" Electronic Frontier Foundation www.eff.org/IP/P2P/howto-notgetsued.php (Accessed 29 July 2008)
[33] See Lahore: "Copyright and Designs" at 51,325 (Butterworths)
[34] Copyright Act 1968 (Australia) S39B (works); S112E (audio visual items)
[35] Copyright Act 1968 (Australia) S36(1A) (works); S101(1A) (subject matter other than works)
[36] US Free Trade Agreement Implementation Act 2004 (Australia)
[37] Section 116AH(1) Copyright Act 1968 (Australia)
[38] 2000/31/EC

The Copyright Act 1968 has also been amended by the Copyright Amendment Act 2006 in order to implement changes to intellectual property legislation necessitated by the Free Trade Agreement signed between Australia and the United States. The amending legislation contains a number of new indictable, summary and strict liability offences which are clearly targeted at those involved in the piracy of copyright material.

A person who creates or operates a P2P platform to enable the unauthorised distribution of copyright material now risks liability under Section 132AC (1), which provides:

132AC (1) A person commits an offence if:

(a) the person engages in conduct; and
(b) the conduct results in one or more infringements of the copyright in a work or other subject-matter; and
(c) the infringement or infringements have a substantial prejudicial impact on the owner of the copyright; and
(d) the infringement or infringements occur on a commercial scale.

Breach of Section 132AC (1) is an indictable offence which carries with it a penalty of up to 5 years imprisonment and a fine of $AUD 60,500 ($AUD 302,500 in the case of a corporation), or both.

It is also possible that those merely using P2P platforms to download or share files risk liability under the new provisions where the downloading or sharing is unauthorised. Section 132AC (3) provides:

132AC (3) A person commits an offence if:

(a) the person engages in conduct; and
(b) the conduct results in one or more infringements of the copyright in a work or other subject-matter; and
(c) the infringement or infringements have a substantial prejudicial impact on the owner of the copyright and the person is negligent as to that fact; and
(d) the infringement or infringements occur on a commercial scale and the person is negligent as to that fact.

Breach of Section 132AC (3) is a summary offence resulting in imprisonment for 2 years and a fine of $AUD13,200. Whether or not a user incurs liability under the section in any instance will very much depend upon whether the court considers that the user was "negligent" as to the substantial prejudicial impact on the copyright owner and "negligent" as to the infringement occurring on a "commercial scale". The section is not particularly well-drafted, and presumably "negligent" refers to the knowledge attributed to the accused about these facts. It is also unclear how "commercial scale" would be defined. The test of negligence is an objective one, and it remains to be seen whether courts will consider as "negligent" the (often unwitting) use of a P2P downloader's computer as a server for future uploads to other users.

In the European context, the European Parliament has called for member states to implement the proposed EU IP Enforcement Directive. The Directive provides for a number of criminal measures aimed at curbing IP violations which occur on a commercial scale[39]. The Directive has been criticised as favouring rights holders to the detriment of their competitors, services providers and individuals[40].

Whilst there is no evidence of criminal prosecutions against users to date, organisations such as the MPA and MIPI have in the Asia Pacific region secured some significant convictions against individuals operating P2P platforms for the unauthorised distribution of copyright material. In October 2006 Chan Nai-ming was convicted and imprisoned by a Hong Kong magistrate for 3 months for distributing three Hollywood motion picture films using BitTorrent software. Chan was prosecuted for breaching Hong Kong's Copyright Ordinance which creates a criminal offence for the distribution of copyright works. Chan's subsequent appeal to the Hong Kong Court of Appeal was dismissed[41].

In terms of convictions for P2P piracy, the high watermark case is from Japan. In December 2006, Isamu Kaneko, the developer of the "Winny" P2P program, was convicted of allowing a large number of Winny users to download copyright material. Whilst the court acknowledged that Kaneko did not actively encourage copyright infringement through use of the Winny platform, he took no action to prevent copyright violations, and knew that many of the files which would be exchanged through the platform would be subject to copyright[42]. Cases such as Kaneko highlight the importance for creators and operators of P2P platforms to take pro-active steps to discourage and prevent unauthorised file-sharing in order to minimise potential civil and criminal liability.

---

[39] Gerard Kelly "Calls Grow for Tougher European Penalties on Piracy", World Media Law Report, March 20, 2008

[40] Ross Anderson "The Draft IPR Enforcement Directive – A Threat to Competition and Liberty" www.fipr.org/copyright/draft-ipr-enforce.html (Accessed 4 August 2008)

[41] "Hong Kong: File-sharing pirate in jail after losing appeal": Asia Media News Daily, Wednesday December 13, 2006 (media article only – no transcript available)

[42] "Winny developer guilty of copyright violations" The Asahi Shimbun, 14 December 2006. www.asahi.com (media article only – no transcript available) (Accessed 29 July 2008)

5. Future Developments

5.1. Litigation against intermediaries

Industry bodies representing rights holders have been successful in shutting down most of the major P2P file sharing platforms including Napster, Gnutella, Kazaa and Grokster. BitTorrent Inc. will probably continue to operate because its business model is centred around the lawful, efficient delivery of large files over the internet and it has not encouraged the unauthorised use of copyright material. Indeed, BitTorrent has recently announced a distribution arrangement with some of the world's leading entertainment studios[43]. But the BitTorrent software is open source and, given its ability to transfer large files at high speed and quality, the software will continue to be used by others for the illegitimate distribution of copyright material over the internet. Some of these illegitimate sites have already been closed down by the MPA[44] but it is inevitable that others will spring up to take their place. In this regard, the P2P genie may be out of the bottle.

Legal action by industry bodies against individual users may continue, but such action is resource-intensive and at best is of deterrent value only. IFPI has recognised the limitations in its strategy of pursuing illegitimate sites and individual users, and now has ISPs and other intermediaries in its sights. IFPI Chairman and CEO, John Kennedy, stated in January 2007:

> "As an industry we are enforcing our rights decisively in the fight against piracy and this will continue. However, we should not be doing this job alone. With cooperation from ISPs we could make huge strides in tackling internet piracy globally. It is very unfortunate that it seems to need pressure from governments or even action in the courts to achieve this, but as an industry we are determined to see this campaign through to the end."[45]

Sure enough, in early 2008 four major recording companies issued proceedings against Irish ISP, Eircom, seeking to restrain the use of Eircom's facilities for the unlawful distribution of copyrighted music. The action was taken after Eircom had refused to adopt filtering technology to monitor and block copyright material which was being unlawfully distributed by Eircom's subscribers[46]. From their own business perspective, it is understandable why ISPs would resist attempts to require them to monitor use and filter content, as this would then require them to incur the cost of taking action against account holders involved in unlawful distribution (not to mention customer alienation, loss of revenue, privacy issues and possible liability in the event of a failure to block particular content).

Another reason why IFPI and other industry bodies may focus on legal action against ISPs and other intermediaries rather than individual users is that in future, individual users may be more difficult to identify and locate. To date, legal action against individual users has been possible because they can be traced through their IP addresses obtained by subpoena of the relevant ISPs. However, new technologies are emerging which enable end users to operate with anonymity and perhaps with even untraceable IP addresses[47].

In their battle against internet piracy, it is inevitable that industry bodies should choose a class of target which is less elusive, more concentrated and usually more pecunious than the individual user. For intermediaries, compliance with "safe harbour" provisions applicable to their respective jurisdictions will become very important in the future in order to minimise their liability.

5.2. Anti-Counterfeiting Trade Agreement and other legislation

5.2.1. The ACTA

In October 2007 the United States, the European Commission, Japan and Switzerland announced a proposal for a new treaty, provisionally known as the Anti-Counterfeiting Trade Agreement (ACTA). The purpose of the ACTA is to establish a new international standard of intellectual property rights enforcement against counterfeiting and piracy[48] and it appears to be the product of lobbying by major rights holders. Whilst a draft of the ACTA is yet to be released and negotiations are being conducted in secret, a leaked discussion paper on the ACTA was uploaded

[43] www.bittorrent.com, media release November 29, 2006. (Accessed 29 July 2008)
[44] Darren Meale & Joel Smith "Downloaders and the entertainment industry – the battle rages", World Copyright Law Report, November 23, 2006.
[45] www.ifpi.org/content/section_resources/digital-music-report.html (Accessed 29 July 2008)
[46] Asher Moses: "Music Industry opens new front on piracy" "The Age" April 25, 2008
[47] Darren Meale & Joel Smith, op cit n 44
[48] Autralian Department of Foreign Affairs and Trade, Discussion Paper "An International Proposal for a Plurilateral Anti-Counterfeiting Trade Agreement" www.dfat.gov.au/trade/acta/discussion-paper.html (Accessed 29 July 2008)

to WikiLeaks on 22 May 2008[49]. Not surprisingly, internet piracy is within the scope of the ACTA, with the discussion paper referring to "safeguards for Internet Service Providers from liability" and "to encourage ISP's to cooperate with rights holders in the removal of infringing material" – which reflects the motivation of rights holders in recent legal proceedings against intermediaries discussed above.

Concern has been expressed that the ACTA will give border guards and enforcement agencies the right to check laptops, iPods and cellular phones for content that breaches copyright laws[50]. Whilst these concerns may be an over-reaction, the provisions in the discussion paper providing for "ex officio authority to take action against infringers" (i.e. authority to act without complaint by rights holders) and "authority to order ex parte searches and other preliminary measures" are cause for some concern.

5.2.2. Other legislation

It is also likely that in response to lobbying by powerful rights holders, some jurisdictions will enact legislation which imposes an obligation upon intermediaries to monitor use and filter content in order to identify infringement.

In Australia there are now plans to introduce legislation which would require ISPs to monitor their users' activities with a view to cancelling the accounts of users engaged in unauthorised file sharing based on a "3 strikes" rule[51]. Such legislation would be regarded by rights holders as being necessary to redress deficiencies in the safe harbour provisions, and will no doubt be resisted strongly by intermediaries. In the writer's opinion the proposed legislation can be seen as part of an on-going tussle between rights holders and intermediaries to allocate to one another responsibility for monitoring infringing use and unauthorised content.

5.3. Usenet

There is some evidence that because of the notoriety of modern P2P platforms for the unauthorised distribution of content over the internet, file sharers are increasingly looking to Usenet newsgroups as a "safer" way to share files[52]. Usenet is in fact a very old (circa 1980) computer communication system involving a loose collection of servers which store and forward files to each other. Articles posted by users to one server eventually find their way to every other server in the network and, unlike P2P networks, are not accessed from the hard drive of the "uploader". Articles posted to Usenet are organised into specific categories or topics called newsgroups[53].

For file sharers, the attraction of Usenet is that, unlike modern P2P platforms where persons distributing content are readily identifiable to other users by their IP address, the origin of a Usenet uploading can be completely obscured once the file has transferred beyond the origin server. For the time being at least, the expectation of anonymity makes Usenet a more attractive proposition for persons seeking to share unauthorised content.

6. Managing Internet Piracy and its Effect

Piracy will never be eliminated, whether it is perpetrated through the internet or through any other means or medium. But piracy and its consequences can be managed. For rights holders, this involves availing themselves of a sensible strategy to protect their content. For users and providers of facilities, this involves taking proper precautions to minimise their liability.

6.1. Rights Holders

6.1.1. Litigation & Enforcement

Legal action against infringing persons will continue to be used by industry bodies representing rights holders, if only for its deterrent value. But such legal action on its own can be a blunt and ineffective instrument and has resulted in considerable bad press for the music industry, particularly in the United States. Increased co-operation

[49] "Discussion Paper on a Possible Anti-Counterfeiting Trade Agreement" http://wikileaks.org/leak/acta-proposal-2007.pdf (Accessed 29 July 2008)
[50] "ACTA trade agreement negotiation lacks transparency". From Wikileaks by Vito Pilieci (Canwest News Services) Monday May 25 2008 http://wikileaks.org/wiki/ACTA_trade_agreement_negotiations_lacks_transparency (Accessed 8 July 2008)
[51] See R. Pulham and S. Stern "Government could legislate to make ISP's monitor their users" World Media Law Report, March 27, 2008
[52] "Internet music pirates find a new patch", The Australian Financial Review, 23 October 2007
[53] Wikipedia offers a useful outline of Usenet

between industry bodies and regulatory authorities may prove to be more effective than litigation against end users, and there has been some movement here.

On December 15, 2006 a number of major industry bodies including the MPA and the Business Software Alliance ("BSA") signed a memorandum with the National Copyright Administration of China ("NCAC") to protect movies, software and other copyright material from piracy via the internet in China[54]. Under the arrangement, the industry bodies will provide the NCAC with details of material which has been produced legitimately for download so that a distinction can be readily made between legitimate and unauthorised content. NCAC has agreed to refer identified breaches to the relevant judicial authority for prosecution.

In July 2008 a Memorandum of Understanding was signed between the United Kingdom Government, major ISPs and rights holders within the music and film industry as part of a government plan for a co-regulatory approach to internet piracy[55]. Under the arrangement, the rights holders and ISPs are required to work together, initially with rights holders identifying infringing use and the ISPs then contacting the relevant users. A similar co-operative scheme championed by French President Nicolas Sarkozy was implemented in France in late 2007[56]. In the writer's opinion, co-operative schemes of such nature are more likely to succeed in curbing internet piracy than a legislative approach as proposed in Australia (see paragraph 5.2.2).

6.1.2. Appropriate Business Models

Piracy may be reduced if rights holders adopt business models which make piracy less attractive. This may involve making content more freely available and accessible online (e.g. by releasing back catalogues on-line), by being realistic in setting pricing structures, and by more innovative product offerings (e.g. delivery of product via USB wrist bands[57]).

6.1.3. Digital Rights Management & Other Technology

Digital Rights Management ("DRM") is the term used to describe various technologies available to rights holders to identify and control access to their material. Identification is achieved by digital watermarking. Digital watermarks enable rights holders to indelibly embed identifiers in digital content which are able to confirm copyright ownership and usage rights. Digital watermarking can have a significant impact on the reduction of internet piracy by improving the ability to monitor, track and manage digital content[58].

Access to content can be controlled by encryption, but as well as restricting, for example, the number of times a legitimately downloaded track can be played, encryption has been used by rights holders to restrict the systems on which that track can be played, including territorial restrictions[59]. This practice by rights holders has quite legitimately raised claims of anti-competitive conduct and, perversely, may even encourage illegal downloading because of the inconvenience often associated with content heavily encumbered with DRM. Customer frustration with DRM has been recognised by the music industry, with EMI recently announcing that it will strip copyright protection from online music sales worldwide[60], and generally there is now a trend within the music industry to offer more unprotected files.

Rights holders can also look to technology to directly combat internet piracy rather than simply manage access to content through DRM. A professor at the University of Tulsa in the United States has developed a program designed to frustrate attempts to illegally download material through BitTorrent. The program creates a flood of decoy or bogus files on the internet which makes it extremely difficult for the downloaders to identify the actual file they have sought to download [61], although obviously this is not satisfactory in respect of legitimate BitTorrent downloads. There are also corporations, such as Media Defender which specialise in piracy protection on P2P networks by creating files which look like pirated movies, software and music, but which do not work when downloaded [62].

6.2. P2P Platform Creators/Operators

6.2.1. Actively Discourage Copyright Breach

[54] MPA News Release, December 16, 2006: "National Copyright Administration of China Sign Anti-Piracy Memorandum with MPA".
[55] See Dugie Standeford "UK Content, ISP Industries Agree to Partner Against Digital Piracy" www.ip-watch.org 28 July 2008 (Accessed 4 August 2008)
[56] "France Unveils Anti-Piracy Plan" BBC news, 23 November 2007 http://news.bbc.co.uk/1/hi/technology/7110024.stm (Accessed 5 August 2008)
[57] Australian Rock veteran Jimmy Barnes has released his new album via a USB wristband which (at a price of $AUD 40) is bundled with other content and which will have further content upload to it over the next twelve months – see "Rocker Rolls on into high tech world without CD's", "The Age" (Australia) July 12 2008
[58] See Digital Watermarking Alliance White Paper www.digitalwatermarkingalliance.org (Accessed 29 July 2008)
[59] See Darren Meale & Joel Smith, op cit n 44
[60] "EMI move means new deal for music downloads" "The Age" (Melbourne, Australia) 4 April 2007
[61] Juliana Torres, op cit n 15
[62] Danny Bradbury, July 8, 2008 www.ft.com "Security Matters: Gunning for the copyright pirates" (Accessed 29 July 2008)

It is evident from the major P2P copyright cases (Napster, Grokster, Kazaa) that the courts found against the defendants because they either encouraged the use of their platforms for unauthorised use of copyright material or were at least indifferent to the fact that their platforms could be used for that purpose. On the other hand, BitTorrent Inc. has been more judicious in the promotion of its platform, and to date has not been subject to legal action by rights holders (as distinct from other operators who have used the BitTorrent open source software with less benign intentions).

In light of the decided cases, it is important for creators or operators of P2P platforms to actively discourage unauthorised use of copyright material. A prohibition to this effect should also be incorporated in the terms of use for the platform.

6.2.2. Adoption of Filtering Software

The operators of the Kazaa system were found liable for authorising a breach of copyright partly because they had the ability to adopt filtering software which would curtail the distribution of copyright material, but failed to do so. Filtering software has recently been incorporated into the Kazaa platform, which now prevents copyright material from being distributed [63].

6.3. Users (Downloaders/Uploaders)

In light of the practice of industry groups representing rights holders to take legal proceedings against individuals involved in file sharing, users must take particular care when using popular P2P platforms. There are a number of initiatives which users can take to minimise risk.

6.3.1. Access files only from legitimate sites

It may not always be easy to confirm the legitimacy of a site which offers music and movie downloads, although with major technology and content owning corporations now entering the downloading market, identification of legitimate sites should become less problematic.

6.3.2. Remove copyright protected files from shared folder

The existence of a copyright protected file in a user's shared folder can expose a user to legal action in the event of subsequent uploading by other users. Whilst this risk can be managed by turning off the "sharing" function on the software, a number of P2P platforms such as BitTorrent do not enable this. Technological assistance is available for users in the form of "Digital File Check", a software application developed by IFPI and MPA[64] which enables users to remove unwanted file-sharing programs and delete copyright protected material from shared folders.

6.4. Content Hosts/ISPs/Carriers

6.4.1. Strong Access Policies/Terms of Use

If intermediaries such as content hosts, ISPs or carriers are to avoid liability for copyright breach by persons accessing their infrastructure, it is important that their access policies or terms of use prohibit users from posting copyright protected material to their sites, or otherwise using their infrastructure as a means of perpetrating a copyright breach [65].

However, access policies or terms of use which prohibit users from breaching copyright will not necessarily satisfy rights holders where copyright in their content has been infringed, and content hosts are deriving very significant advertising revenue from sites which host such material. In March 2007, Viacom filed a lawsuit in the United States against YouTube and its parent company Google (probably in response to Google's delay in implementing filtering technology), alleging intentional copyright infringement by YouTube, and claiming more than $US one billion in damages [66]. The litigation now has significant privacy implications. In July 2008 a United States District Court ordered Google to give Viacom log in names of YouTube users and internet protocol (IP) addresses identifying which computers they used for viewing videos [67].

---

[63] See Michael Williams op cit no. 27 at pag 84.
[64] Discussed by Joel Smith in "Is film-sharing the new P2P? How Hollywood is facing the challenge." World Copyright Law Report, November 10, 2006.
[65] See, for example, the YouTube Terms of Use at www.youtube.com/t/terms (Accessed 29 July 2008)
[66] Anne Broache and Greg Sandoval "Viacom sues Google over YouTube clips". March 13, 2007 CNET News.com at http://news.cnet.com (Accessed 29 July 2008)
[67] "Google Ordered to Reveal YouTube User's habits", "The Age" July 5, 2008.

6.4.2. Filtering Technology

Rights holders have been exerting considerable pressure upon ISPs to adopt filtering technology to monitor use and block the transmission of unauthorised content. However, it is doubtful that network-level filtering technology is at a stage of maturity which allows ISPs (acting as conduits only) to effectively identify and block transmission of unauthorised content, and in any event not where the content is encrypted. But this may change – academics from Tsinghua University in Beijing, China, claim to have invented an intelligent filtering system for P2P networks which identifies authorised content and blocks illegal file distribution (even where files are encrypted) based on file signatures automatically generated by the filtering systems [68]. The system claims to block 85% of unauthorised files.

6.4.3. Safe Harbour Provisions

An intermediary may be able to limit liability for copyright breach by a user of its infrastructure if the intermediary is subject to "safe harbour" provisions which may operate in the jurisdiction of the intermediary. As discussed above, the Australian "safe harbour" provisions apply only to 'carriage service providers' under the Australian Telecommunications Act 1997. The "safe harbour" provisions of the United States Digital Millennium Copyright Act 1998 ("DMCA") appear to extend to any website which hosts material posted by third parties, as well as other platforms which enable third parties to post or distribute copyright protected material [69].

As previously observed, "safe harbour" provisions have been criticised by rights holders for facilitating piracy, but they have also been subject to criticism by intermediaries, particularly in the United States where the DMCA provisions have allowed intermediaries to be bombarded by computer-generated claims which are often inaccurate. However, such provisions can offer intermediaries very significant protection in the event of copyright infringement or piracy effected through their infrastructure. In light of increased litigation by industry bodies against ISPs [70], intermediaries cannot afford not to take advantage of such provisions if they are available to them.

7. Summary

Because of its de-centralised nature, the ability to efficiently transfer very large files and the availability of open-source file sharing platforms, P2P computing creates an environment where copyright piracy can proliferate. However, it seems likely that in many jurisdictions a bona fide platform can be created without subjecting the creator or operator to copyright breach.

Legal action against end users by rights holders is not always effective in fighting piracy. Rights holders must set realistic expectations for intermediaries, adopt new business models for distribution of their material so as to reduce the incentives for unauthorised use, and use technology sensibly in order to manage their rights.

Users will remain targets for legal action by rights holders and will need to exercise care in accessing copyright protected material. In particular, they should ensure that they access material only from legitimate sites.

Intermediaries such as content hosts, ISPs and carriers are more financial and less elusive than pirates and end users, and must prepare themselves for future litigation by rights holders. They must also be prepared to co-operate with rights holders in dealing with infringing use, or they can expect any applicable "safe harbour" provisions of their jurisdiction to be watered down. The financial and political muscle of the more powerful rights holders will surely see to that.

JOHN LAMBRICK
6 August 2008

[68] Liu, Ning, Xue and Wang: "PIFF: An Intelligent File Filtering Mechanism for Peer to Peer Network" http://ieeexplore.ieee.org/iel5/4030851/4030852/04030897.pdf (Accessed 29 July 2008)
[69] Alan Lewine "Digital Millennium Copyright Act. The Service Provider Safe Harbour Under 17 U.S.C. 512": http://lewinelaw.com/DMCA512Update.htm (Accessed June 2007)
[70] See note 45 ante.