Online Intermediaries and Liability for Copyright Infringement

Lilian Edwards and Charlotte Waelde[1]

Contents

[1]Co-Directors, AHRC Research Centre for Studies into Intellectual Property and Technology Law, School of Law, University of Edinburgh; email L.Edwards@ed.ac.uk. Charlotte.Waelde@ed.ac.uk. Our thanks to Jun Gu for research assistance.

A. Outline

Ascribing liability for infringement of copyright in works disseminated over the Internet without authorization has been a most vexed issue over recent years. Barely a day passes without a news story detailing the attempts of the entertainment industry to exert control over dissemination of content in which it owns copyright, matched by stories discussing technical breakthroughs enabling content to be passed between Internet users with ever greater ease and speed. Could, or should, those who author and disseminate the programs which facilitate infringement of copyright be held to account for the underlying infringements by their users? Might the standards developed over the years for ascribing liability to the more traditional forms of online intermediaries and thereafter, subject to conditions, shielding them from liability, present an appropriate framework for this newer type of intermediary which develops and distributes the means by which user can infringe copyright? Where might an appropriate balance lie between the content owners' search for profitability, and the pressing interest in seeing technology develop apace?

The purpose of this scoping paper is to confront these issues. In so doing we will:

- Address the concept of an "*online intermediary*" and how far it has moved in general online intermediary immunity law from the traditional, more restrictive, concept of an ISP;
- Discuss how *general or "traditional" intermediary immunity law* has evolved, with reference to

leading examples from various legal systems. In particular, we will focus on the idea of "notice and take down" (NTD) regimes, and the problems they raise in the copyright area in relation to freedom of expression, privatised censorship, public scrutiny and the public domain;

- Examine how the *liability of P2P intermediaries for copyright infringement* has been addressed globally and how different the law is in this area from the "general" immunity law approach. In particular, we note that the NTD paradigm and the "safe harbors" for intermediaries set up by both EU and US law are inappropriate to protect post-Napster decentralized P2P intermediaries, insofar as they fulfill socially beneficial functions by distributing substantial amounts of non-infringing content;
- Consider what transpires if an intermediary *cannot* be identified who is liable in law for the upload/download of files shared using P2P systems. Increasingly, record and film industry associations such as the Recording Industry Association of America (RIAA), the Motion Picture Association (MPA) and, in the UK, the British Phonographic Industry (BPI), *have begun suing individual users* for direct copyright infringement. This approach, however, raises two problems that we will address:
  - first, in many jurisdictions private non-commercial copying is legal, albeit usually backed by a levy system, for example on blank recording media (CDs, tapes) and/or recording equipment (CD/DVD player-recorders). How does this affect liability for file sharing? We examine in particular the implications of systems like BitTorrent where by default every downloader is also an uploader.
  - second, in these cases, the user is nearly always file-sharing using a pseudonym (or, on some systems, such as Freenet, entirely anonymously) and so it is necessary to make a request for disclosure of the user's true identity to the user's ISP, before any legal proceedings can be effectively commenced. This sets up a further aspect of "online intermediary liability": is an ISP or host required to make such disclosure, and if they do, what are the implications for the general privacy rights of users? How, for example, do duties of disclosure, if imposed, cohere with duties not to disclose personal data relating to living persons under EU data protection regimes? This issue, once seen as tangential to the main thrust of P2P cases, has become of increasing public concern as a deluge of actions has been instigated against individual users of P2P software. In the final section of this paper, we will thus examine briefly the early, rather scattered, trends emerging in this area of anonymity and disclosure.
- Explore whether the current legal assault by the content industries on P2P intermediaries is the only alternative to safeguard the legitimate rights of creators and publishers to a revenue stream for use of their works, and briefly examine *alternate business models* such as levies, DRMs, and legal commercial file downloading services; and

- Finally, we ask if the right balance is being struck between the rights of authors and content providers and the need not to restrict the development of technologies such as P2P as a public good.

B. Introduction: themes and issues

The problem of liability of online intermediaries on the Internet was one of the earliest problems in the cyberspace environment to grab headlines, worry the fledgling Internet industry and demand the serious attention of lawyers[2]. Early cases mainly originated in the USA and focused on the liability of large Internet Service Providers (ISPs) such as AOL or CompuServe for hosting, transmitting, or publishing material that was in some way criminal or civilly actionable: notably libellous, defamatory or pornographic content[3]. Liability issues arose in the context of many different types of content and might raise different issues depending on the type of content. As well as those discussed above, disputes have been reported involving material which is in contempt of court [4]; material to which privacy rights apply (for example, the *Estelle Halliday* case in France[5]); material which is blasphemous [6]; *et al*. Surprisingly, very few of the early cases involved copyright infringement and many of those that did were primarily brought by the Church of Scientology protecting its sacred texts from disclosure to the public, rather than, as might have been expected, by commercial interests such as book, music or film publishers.

As we shall see below, legislation has sometimes been introduced to deal with online intermediary liability in relation to particular types of content (the UK Defamation Act 1996, the US Digital Millennium Copyright Act ("DMCA")) - which we will term a *vertical approach* to legislation; while other legislation is intended to provide immunity in respect of all, or at least a range, of different types of content liability – an approach known as *horizontal*. The best known example of comprehensive regulation in the horizontal category is the EC Electronic Commerce Directive

---

[2] *Cubby v CompuServe* 766 F Supp 135 (SD NY 1991), a libel hosting case, was one of the earliest cyberlaw cases of any kind to be decided, in 1991. A Dutch prosecution of an ISP for hosting copyright material was also reported in 1991 (see Oosterbaan DTL *et al* "eCommerce 2003: Netherlands" in *Getting the Deal Through: eCommerce 2003 in 25 Jurisdictions Worldwide* (Law Business Research Ltd, 2003).

[3] For historical context, see earlier discussion of these issues by this writer in Edwards L. "Defamation and the Internet" and "Pornography and the Internet" in Edwards L and Waelde C eds. *Law and the Internet: A Framework for Electronic Commerce* (Hart, 2000).

[4] See *R v Barnardo* [1995] Ont. C.J. Lexis. In the UK in 2001 the ISP Demon successfully asked the courts to grant them an exemption from strict liability for contempt of court; this arose in relation to their fear that they would inevitably be involved in illegal pre trial publicity relating to the "Jamie Bulger" Thompson and Venables murder trial: see http://www.guardian.co.uk/Archive/Article/0,4273,4222156,00.html.

[5] Tribunal de Grande Instance de Paris, 9 June 1998. See summary at http://www.kahnlaw.com/usa/newsjob/publications/french_isp_cag_dg.htm.

[6] See unreported 1997 UK case involving gay poem found illegal as blasphemous in the UK courts ; a host in the UK subsequently linked to that poem (which was hosted physically on a server abroad) and was reported to the police for so doing. A police investigation followed but no charges were to this author's knowledge ever brought. Details at http://www.xs4all.nl/~yaman/linkpoem.htm.

2000[7] ("ECD"), examined in detail below.

Problematic content can also be categorized by who originates or authors it, and their relationship with the online intermediary. This is significant because, where a contractual relationship exists between author and intermediary, risk can at least partially be controlled by contractual penalties and indemnity clauses. Where no contractual nexus exists, risk is worryingly indeterminate. Content may, for example be originated by a party with whom the ISP had a contractual relationship, as in the typical example where a consumer signs up to a standard ISP for a monthly sum, who agree to give him around 5MB of space where he can set up his own website; it may be provided by a third party with no contractual nexus with the ISP, as where a newsgroup posting which is alleged to contain illegal pirate "warez" is transmitted by the ISP as part of its standard "feed" to customers; or the content may be originated by the ISP itself as part of its service to its customers.

The different issues of policy raised by these different classifications of authorship and types of content were largely not teased out systematically in the early jurisprudence, leading to widely differing regimes being imposed both in different legal systems and within the same legal system but in differing scenarios, depending on the type of offending content in question. Early case law also referred unsystematically to "ISPs", "bulletin boards", "online publishers" and similar terminology. This lack of harmonisation in the emerging case law led to calls from industry for some form of rescuing certainty in the form of special statutory regimes from as early as the mid 1990s. As discussed below, over time, the debate over liability for online intermediaries came to be seen less as tied to different types of *content* – libel, pornography, material infringing copyright, material invading privacy – and more as a holistic problem of whether *intermediaries* on the Internet should in general be made responsible for the content they made accessible to the public, transmitted or stored.

- At the same time, the issue of liability for content became a major worry not just for the relatively small traditional ISP community – the Yahoo!s, CompuServes and AOLs of this world - but also for a wide spectrum of newer types of Internet intermediaries involved in the hosting, storage or transmission of information; including but not restricted to: online sellers and distributors of goods and services, virtual and non-virtual eg Amazon, Tescos Online, CDNow, dating websites; online auction sites such as EBay, QXL and Yahoo!;
- "portal sites" - often, though not exclusively former plain "ISPs" expanding to fulfill a wider intermediary role and providing one-stop access to eg weather reports, news, entertainment, horoscopes, auctions, game and software downloads, diary software, etc. Largely seen as

[7] 2000/31/EC, passed 8 June 2000.

replacing the earlier concept of "virtual shopping centres" or "virtual malls";

- software and game providers like Microsoft, Sun, Nintendo, who often make either whole computer programs or bug patches available for download online;
- virtual information providers eg, *The Register, Slashdot,* often providing interactive fora and moderated or unmoderated comment facilities;
- aggregators - sites which provide links to a variety of sites so that, say, a user can read the headlines from multiple news sites conveniently on one web page;
- traditional media organizations going "digital" such as BBCi, *New York Times, Wall Street Journal;*
- universities;
- libraries and archives offering access to digitised content;
- search engines or "locational tools" (cf DMCA)
- chatrooms;
- "webblog" or online diary sites, eg Moveable Type, Blogger, LiveJournal;
- mailing list moderators; and
- individuals and institutions setting up websites which involved content provided by a third party or hyperlinks to such content.

Liability worries also came to affect a wider range of Internet communications intermediaries than just traditional telephone companies, such as

- Internet backbone providers,
- cable companies, and
- mobile phone communications providers.

In consequence, the early sharp distinction drawn basically between Internet Access Providers (IAPs) - who merely provided "*fundamental communications services such as access, information storage etc*", and Internet Service Providers (ISPs), who provided "*some additional service which facilitates a transaction between end users, eg identifying one of the parties, providing search facilities etc*"[8] became less and less meaningful as the ISP sector expanded during the boom years of the Internet to provide portal services giving access to large amounts of both in-house and third party produced content, while providers of what might be seen as "pure" telecommunications services, like mobile phone companies, also became deeply involved in both the "content business" and in providing "value added" services such as locational data handling. The issue became increasingly whether a regime

[8] Reed C *Internet Law: Text and Materials* (Butterworths, 2000), Chapter 4, p 78.

should be devised providing immunities for some class of "online intermediaries" wider than ISPs.

In the field of copyright liability, in particular, new classes of "online intermediaries" have emerged which were largely not in the minds of legislators at the time of drafting of leading immunity instruments in the late 1990s, such as the EC Electronic Commerce Directive (ECD) and the US Digital Millennium Copyright Act (DMCA). These have arisen in the wake of the extensive promulgation and use of peer-to-peer (P2P) file sharing software programs, such as Napster, Grokster, EMule, SoulSeek and BitTorrent (to name but a few). The various immunity provisions or "safe harbors" in instruments such as the ECD and DMCA were largely designed not to deal with copyright infringement in the context of P2P intermediaries, but to address more straightforward situations of transmission, caching, and hosting of content. A typical situation envisaged was where a traditional ISP made file-space available to a subscriber on its server and, unknown to the ISP, that subscriber used that space to download, store and possibly upload illegal copies of copyright works. Here the ISP is fairly clearly a "host" without awareness of providing access to infringing works and, unless put on notice (also discussed below) was exculpated from civil and criminal liability under both the ECD and DMCA regimes.

But in the brave new world of peer-to-per (P2P) file-sharing, a number of "new" intermediaries less obvious than "hosts" can be identified, which have to some extent come to the attention of the courts. These, as discussed in more *legal* detail at p 38 below, are the intermediaries who enable or assist in the downloading and uploading of files, both legal and illegal, by means of particular P2P software. These intermediaries include the actual writers of the P2P software, and the web sites from which P2P software can be downloaded by users (distributor sites). In the case of BitTorrent ("BT" - see below) three types of intermediary are involved apart from the actual writers of the various BT clients: torrent sites, "trackers" and "seeders". These will hereafter be described globally as *"P2P intermediaries"* but obviously, distinctions may need at points to be drawn.

P2P intermediaries do not themselves typically host files of any kind which infringe copyright (cf, early "simple download" sites such as MP3.com, where the site itself was a host and clearly a primary infringer of copyright). Instead, P2P intermediaries usually enable users who have downloaded particular flavours of P2P software to then *inter se* unlawfully swap and share files containing works protected by copyright. Conceptually, they are best seen as "pointing to" infringing material rather than directly hosting it or transmitting it. There are three or four clear variations on this theme.

First, the P2P intermediary, on its own website, provides a *centralised index* to all the files stored and available for upload on the various users' individual computers. This model, which

typically provides the most speedy and efficient search facilities for users, was that used by the now defunct pre-commercial Napster site which was, mainly on this basis, found liable for contributory and vicarious infringement of copyright (see below).

The second model, which is now the default approach following the Napster lawsuit, is that such a centralised index is *not* made available. Each user instead maintains an index only of those files stored on his or her own machine. A user searching for a particular file "traces" a desired file by sending out a request which is passed from user to user of the P2P software in question, until it is met with a positive response, after which the file download is negotiated by the software between the user who has the file and the user who made the request. This decentralised, slower model is that used by P2P services descended from Gnutella such as KaZaA and Grokster and has so far proved safer from legal challenge (though see also below).

A third approach which is merely a variation on the above, is that although there is still no centralised index, a number of user computers ("supernodes") act as servers hosting sub-indexes, thereby speeding up search times. Such "supernodes" can be seen conceptually as "sub-Napsters".

A fourth approach, which is gaining popularity and is now used in more than half of all downloads , is the "BitTorrent" approach. BitTorrent traffic made up 53% of all P2P traffic in June 2004[9]. This is very different from the intermediary architectures described above as it is not a pure P2P application. Users of BT find lists of "torrent" sites using ordinary web sites such as The Pirate Bay, not by using search facilities built into whatever BT client they have downloaded. In simple terms, a particular file is not just downloaded by one user A from just one other identified host/user B, but instead it is fetched from any other user who is sharing that file. Not only that, but the file is split into parts, each of which can be transferred independently, so that user C may be sharing the second half of a file while they download the first part, while user A is doing the opposite, each of them supplying the part the other lacks. In fact this can scale up to hundreds of users downloading files that may have thousands of parts.

This improves transfer speed enormously by transferring the load from a single source to a distributed cloud of sources, so that the system is very useful for handling very large files such as movie files as well as large files such as Linux system software. The BitTorrent approach means that it is difficult or impossible to identify any one file as having been copied directly from any particular single user, which complicates the copyright situation further. So far the legal challenges have centred on 'trackers' (central computers which keep track of all the users downloading a particular file and allow them to find each other) and 'seeders' (users who leave the file available for sharing after they have finished downloading it)[10]. "Torrent" files themselves contain no copyright content

[9] Parker A "The true picture of peer-to-peer filesharing", 2004, at http://www.cachelogic.com/.

[10] There is almost no point in suing or otherwise demanding take down of the sites from which the BT clients themselves can

but merely point the would-be downloader towards a "tracker" site or computer. Every downloader using BitTorrent is also likely by default to be an uploader, something which may be significant in civilian legal jurisdictions such as France where downloading for private non-commercial purposes may fall within a legal exception to copyright. A recent variation on a BT client is EXeem, which combines BT with true P2P technology so that there is no need for web sites such as The Pirate Bay to find torrent files. This removes one class of obviously liable intermediary.

Finally a system which so far has reputedly gathered over 2 million users despite being in many ways still a research project and slow to use, is Freenet[11]. Freenet loosely resembles BitTorrent (though operating on a very different protocol), in that files are downloaded and uploaded in small chunks from multiple sources, rather than as a whole, but is optimized further to reduce both the knowledge and thus the liability of the parties involved in file-sharing. Files are encrypted so that even a host sharing a file (or a chunk thereof) cannot identify what the file is he/she is uploading or storing. Thus, even if an offending file is tracked down to a particular PC, there is no way for investigators to know whether it originated there, or if it was forwarded from another node, or from 300 other nodes before that, on the network. For this reason it is suspected that Freenet is ubiquitously used to share child pornography image files, since it may provide strong defences to users accused of possessing or distributing such images. It is an interesting legal question if a Freenet user found to be unauthorisedly in possession of (parts of) copyright files such as MP3s could possibly be successfully sued.

It is worth noting that the shift from the first type ("Napster" intermediaries) to the later more complex configurations has largely been driven by the desire to escape legal liability[12]. Computationally, the move has on the whole been from more to less efficient architectures, in terms of speed of downloading and search efficiency. BitTorrent, however, is decentralised for other reasons than avoiding legal risk, and is a very efficient way to distribute and retrieve large files. By contrast, Freenet is almost wholly anonymised and decentralized, but is extremely awkward to use for the ordinary consumer.

It is one of the oddities of the copyright domain, compared to, say, intermediary libel liability, that

---

be downloaded – the equivalent of the central Napster or KaZaA sites attacked in their respective lawsuits – as BT is an open source project and so new sites would simply be put up instead. In any case, as discussed above, control of the BT network lies with the "tracker" and "seeder" sites, not with the BT client authors. See Lyman J "Legitimate use, open source, keep BitTorrent out of court", *Newsforge*, March 1 2005 at http://trends.newsforge.com/article.pl?sid=05/03/02/1748210&from=rss .

[11] See Roemer R, "The Digital Evolution: Freenet and the Future of Copyright on the Internet" 2002 UCLA J.L. & Tech. 5 at http://www.lawtechjournal.com/articles/2002/05_021229_roemer.php .

[12] P2P software developers are very well aware that legal liability is now vital input into their technical specification : see F. von Lohmannn "IAAL: What Peer-to-Peer Developers Need to Know About Copyright Law" at http://www.eff.org .

what we might call the "general" laws as to online intermediary liability - the DMCA, ECD type rules - have in general been applied only to "traditional" intermediaries such as ISPs and universities in relation to content which infringes ; while the newer "P2P intermediaries", when sued for assisting in copyright infringement, have either not plead these immunities or, in the cases of *Napster* and *Aimster* (see below p 43), have been denied access to general online intermediary immunities or "safe harbors"[13]. Instead, these cases have largely been fought on the principles of contributory and vicarious liability for infringement of copyright, as discussed below.

C. Online intermediaries – ISPs, IAPs, ISSPs or online intermediary service providers?

The earliest piece of legislation tailored to deal with online intermediary liability is probably the US Communications Decency Act 1996 (CDA). The CDA expressly excluded any effect on intellectual property law, including intermediary liability – which is now dealt with by the DMCA – but it is still interesting as a baseline for the concept of an online intermediary. Section 230 (c) provided that "*no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another content provider*". An "*interactive computer service*" was 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 and such systems operated or services offered by libraries or educational institutions.*[14]" There is a clear emphasis here, it seems, on Internet *access* providers as opposed to Internet hosts or service providers. However s. 230(c) has also been successfully invoked several times to claim immunity by websites[15]; and also by the moderator of a website and mailing list in *Batzel v Smith*[16] (who, if not the "provider" of an interactive computer service, was certainly the "user"). More recently however, an online auction site was found in *Grace v EBay*[17] *not* to gain the benefit of s. 230(c), as it was distributing rather than publishing content provided by a third party. This decision implicitly limits the intermediaries protected to publishers rather than distributors of online information. The CDA is thus typical of early statutes in providing a definition probably intended to cover only the traditional ISP sector but capable of wider extension by favourable judicial interpretation. Many early developing country statutes adopt similarly, fairly vague and inclusive terminology, eg the Singapore Electronic Transaction Act 1998, s. 10[18] refers to a "network service provider" which is not explicitly defined further; the Indian

---

[13] See *A & M Recordings, Inc. v. Napster, Inc.*, 2000 WL 573136 (N.D. Cal. May 12, 2000); *In Re Aimster* 334 F.3d 643.
[14] Section 230(f)(2).
[15] *Carafano v. Metrosplash.com, Inc.*, 207 F.Supp.2d 1055, 1065-66 (C.D.Cal. 2002).
[16] 333 F.3d 1018. This was a controversial decision, with a minority dissenting opinion taking the position that s. 230(c) was *not* intended to cover an individual who deliberately republished the work of a third party (an email sent to the moderator of a Museum mailing list) without checking first if it was intended for publication, and that it was free of actionable content.
[17] 2004 WL 1632047 (Cal. App. 2nd Dist. July 22).
[18] See full text at n 65 infra.

Information Technology Act 2000[19] also refers to "network service providers" which are then (not very helpfully) defined further as "intermediary".

Moving forward, a service provider under s. 512 of the later and more carefully drafted US Digital Millennium Copyright Act (DMCA) is defined either as "*an entity offering transmission, routing, or providing connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received*" or, more widely, "*a provider of online services or network access, or the operator of facilities thereof*" (s. 512(k)(1)(A-B)). This broad definition appears to embrace traditional ISPs, search engines, bulletin board system operators, and even auction web sites. However as discussed below, the US courts have refused to extend these safe harbor provisions to the Napster software program and service, and to a similar system known as Aimster, leaving open the question of whether P2P networks can ever qualify for safe harbor protection under Section 512.

Articles 12-15 of the EC E-Commerce Directive[20] (ECD) introduced in 2000 a regime dealing with the liability of intermediaries throughout Europe. The regime is very widely drawn, affecting not just ISPs but "ISSPs": "information society services providers"[21] or, as the title of Section 4 of the ECD also calls them, "intermediary service providers". An "*information society service*" is defined[22] as "*any service normally provided for renumeration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service.*" "Recipient of a service" is defined[23] as "*any natural or legal person who… uses an information society service…*". Thus, broadly, the ECD intermediary service provider liability regime covers not only the traditional ISP sector, but also a much wider range of actors who are involved in selling goods or services online (eg, e-commerce sites such as Amazon and Ebay); offering online information or search tools for revenue (eg, Google, MSN, LexisNexis or WestLaw); and "pure" telecommunications, cable and mobile communications companies offering network access services. However the requirement that an information society service be offered "at the individual request of the recipient" means that TV and radio broadcasters do not fall within the remit of the ECD liability regime, although sites which offer individually on-demand services such as video-on-demand or email are included. In particular,

---

[19] See Indian IT Act 2000, s. 79. "For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention. *Explanation*.—For the purposes of this section,— (a) "network service provider" means an intermediary; (b) "third party information" means any information dealt with by a network service provider in his capacity as an intermediary;"

[20] 2000/31/EC, passed 8 June 2000.

[21] Art 2(b), ECD. These providers can be natural or juristic persons.

[22] Art 2(a) of the ECD refers back to the definition in Art 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC. The definition is discussed further in recitals 17 and 18 of the ECD.

[23] Art 2(d), ECD.

spammers and other "providers of commercial communications"[24] are included as providers of information society services.

Importantly, recital 18 of the ECD notes explicitly that although a service may be free to the recipient, this does not mean the provider of that service need fall outside the scope of the ECD if the service broadly forms part of an "economic activity": so, arguably, providing non-commercial services online, such as the delivery of e-government services by state departments, falls within the ECD regime if the state will be making economic gains out of the activity (eg, if they are cutting costs by putting service delivery online). It also seems uncontroversial that companies such as Google, which provide its search engine free to the public, but which service has helped it to create an extremely successful business which makes revenue in other ways, should benefit from the immunities granted by the ECD regime. If Google did not so benefit, it might be tempted by the risk-benefit analysis to stop offering its services for free, to public detriment. Given that one of the dominant successful models of e-business is to give away a major product or service but then make money out of it in lateral ways (the "Netscape" effect), it would be unhelpful for the future development of online business if the definition of an ISSP was to be interpreted in any more restrictive way.

Recital 18 of the ECD provides that certain relationships are excluded from ISSP status as not provided wholly "*at a distance*": an employer, for example, is not a provider of an "information society service" in terms of his employment relationship with his workers, it seems (even if they work for him exclusively down a broadband line from home, using databases hosted on the business's server?); a doctor is not a provider of such a service (even if he bills his private clients and sends them their prescriptions exclusively by email?), so long as his advice even partially requires the "physical examination of a patient". This may raise some awkward questions not anticipated in recital 18's examples. What if an EU-situated university server provides personal workspace to all students attending regular classes, and unauthorized copies of MP3 files are found on the university server which have been downloaded by an undergraduate student? The relevant record company association then claims the university is liable. Whatever the basis of copyright infringement alleged, at first instance this seems clearly in policy terms a case where the university should obviously be regarded as an ISSP within the ECD framework, and thus fall within the hosting immunity described in more detail below. Yet although the university does indeed run a server which delivers an "information society service", at a distance, to students, it *primarily* fulfils its role, providing educational services to this student, by *face to face* education rather than distance learning. Should and

[24] See further recital 18, ECD.

will it be regarded as an ISSP for the purposes of hosting immunity?[25] Should a distinction be drawn between the university's hosting activities as a normal provider of face to face studies, and as an entrepreneur providing a distance learning programme to students who *only* interact with it at a distance? The answers still seem likely to be, respectively, yes and no, but the implications need consideration. Since almost every commercial and public institution is soon likely to maintain a website or database, for some if not all purposes connected to their function, this will effectively extend the immunities of Articles 12-15 far beyond the traditional "electronic" sector, and even beyond all information publishers and online sellers, to every institution that hosts content provided by parties other than itself.

D. Anxieties around intermediaries and liability for copyright infringement: history

There have been no reported UK cases to date, and surprisingly few global ones (those few often involving the Church of Scientology as vigilant plaintiffs) dealing directly with Internet intermediary liability for hosting or distributing infringing material[26]. However the potential risk for intermediaries is so great given the volume of potentially copyright-infringing material distributed and hidden on the Internet, that this is now perhaps the main issue driving the development of intermediary liability law worldwide. In the 1990s, the main worry ventilated for ISPs relating to intellectual property (IP) infringement was potential liability for "caching" - a ubiquitous technical process whereby local copies of remote web pages are made by hosts when requested, in order to speed up delivery of those pages on subsequent request. It was initially uncertain if such activity would be construed as making unauthorised copies of copyright work. To some extent, national implementations of the 1996 WIPO "Internet Treaties", the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT) have addressed this particular question[27]; but anxiety about caching has given way to general concern about liability for the vast amount of unauthorized music, software and movies available on the Internet. Such content often exists without the knowledge either of the Internet access provider who gives access to it, or, more pressingly, the host whose servers it sits on. (A traditional ISP often plays both roles as most

[25] Interestingly, the US DMCA specifically gives safe harbor to universities for items posted by their students or staff – see 512(e) – rather than leaving them to rely on the more general safe harbors. See *infra*.

[26] "Indirect" copyright infringement cases involving the liability of sites distributing peer-to-peer software which assists in illegal downloading are, as discussed below, a slightly different kettle of fish, though they do clearly have some relevance in the domain. See the discussion of global trends and cases relating to ISP and P2P liability, infra at p 38.

[27] See in Europe, EC Copyright Directive 2001/29/EG of the European Parliament and the Council of 22 May 2001, article 5(1) which includes as an exemption from the exclusive right of reproduction of the author, "temporary acts of reproduction which are transient or incidental and part of a technological process whose sole purpose is to enable (a) a transmission in a network between third parties by an intermediary and (b) a lawful use of a work or other protected material. There are still doubts that the provisions of the EC Copyright Directive and the ECD on caching are entirely reconcilable: see van der Net "Civil Liability of Internet providers following the Directive on Electronic Commerce" in Snijders H and Weatherill S. *E-commerce Law (*Kluwer, 2003) at p 53.

consumer and business ISPs provide host space of a fixed or negotiable size to customers. Universities similarly tend to be exposed to this dual risk.) The explosion in illegal downloading and filesharing via peer-to-peer (P2P) networks such as the (now defunct) pre-commercialised Napster, KaZaa/Morpheus, EMule and AudioGalaxy[28] has only exacerbated the concerns of intermediaries at their exposure to risk. Not only do ISPs and hosts now have to consider if they may be held liable for hosting pirate material of whose existence they may be entirely ignorant, but also if they potentially may be liable for hosting or giving access to software used to *enable* illegal file-sharing and downloading by third parties. The US DMCA introduced detailed provisions in Section 512, which largely exempt ISPs in the USA from liability for hosting copyright infringing material, but only on certain terms, such as the disclosure of the identity of infringers on request, and subscription to a detailed code of practice relating to notice, "take-down" and "put-back"[29]; we discuss these rules further below.

A key question which remains under-explored in worldwide legislation (although it is addressed in the DMCA) is whether an intermediary, which provides a hyperlink to a site where illicit content is available, is liable for that content. The point is a vital one, not just because hyperlinking is the lifeblood of the Net, but because hyperlinks to unknown sites of unknown content are generated automatically by locational tools such as search engines every time a user requests a search[30]. As noted above, given that search engine technology is vital to use of the Internet and is generally provided for free to most users, it would seem important to avoid placing unreasonable burdens of potential liability on search engine providers in respect of content to which they link. Current legal advice for those building commercial websites is now not only to disclaim liability for content linked to, but also frequently to seek to avoid any risk by requesting permission to link, on the grounds that linking might somehow equate to making, or authorising the making of, an illegal copy; whatever the law says here (which is unclear and will vary from jurisdiction to jurisdiction) this could prove to be an unfortunate practice in policy terms as it restricts Internet growth and connectivity, and may encourage extortionate demands from the site to which the request is made.

E. Policy issues in constructing general legal regimes for online intermediary liability

The rise of intermediary immunity: ISPs and the retreat from Prodigy

[28] See as a brief introduction to P2P technologies, downloading and the law, Guadamuz A . "Music Downloading: the basics " at http://www.law.ed.ac.uk/ahrb/publications/online/downloads.htm and accompanying Powerpoint presentation at http://www.law.ed.ac.uk/ahrb/publications/online/musicdownloads.ppt.

[29] See further p 24 infra.

[30] The early Scottish case of *Shetland Times v Shetland News*, 1997 SLT 669, broadly explored the question of whether hyperlinking constituted copyright infringement, on the rather odd ground that it might constitute unauthorised tapping of a cable programme service, but failed to reach a determinative conclusion. UK law on this point has in any case since been amended. See further MacQueen H "Copyright and the Internet" in Edwards and Waelde eds *Law and the Internet* (Hart, 2000).

This section discusses the policy background to the evolution of what we term “general intermediary liability regimes”. These include both horizontal and vertical legislative approaches, but regard the problem of liability of online intermediaries as a discrete legal question. Much of the development in this area has been driven by cases involving liability for defamatory or pornographic material: nonetheless this is still relevant to understanding what has driven the eventual wide scope of immunities granted by instruments like the DMCA and the ECD to intermediaries.

The classic starting point when exploring intermediary liability is to note that the Internet is a unique medium where no content author or provider can, in general, publish or distribute material on the Net without the aid of an Internet *access* provider. This immediately put the emerging industry sector of ISPs on the spot as star defenders in early Internet liability cases. In the UK and the US, the attractions of suing an ISP as publisher in preference to the original content author or provider speedily became apparent in early Internet libel cases - since the ISP was likely to be locatable, with a registered place of business, and probably with significant liquid assets (a “deep pocket”). By contrast, the original author/provider might have vanished, acted under the cover of anonymity or pseudonymity, be living in another country where judgements for damages were difficult or impossible to get recognised and enforced, or simply have no attachable assets. As a result, traditional ISPs, by virtue of their role as gatekeepers to the Internet, have long felt themselves to be sitting on a liability time-bomb.

These concerns may be heightened when taking into account the nature and quantity of the content which some online intermediaries typically host, transmit or distribute. A commercial ISP usually allows its subscribers access both to read and write to newsgroups or local forums, chatrooms, mailing lists and the millions of Web home pages. It may also give them space to host their own local content. Internet content is often not static but may change from minute to minute, as in chatrooms or online diaries. This scenario generates far too much material to be manually checked and supervised for potentially illegal or actionable content. In comparison, the “real world” hard copy publisher – such as a newspaper or book publisher - can generally feasibly check what they publish each day (and get their lawyer in to make sure in difficult cases). Furthermore, as noted above, intermediaries often give access to, host and transmit content originated by third parties with whom they have no contractual relationship, while hard copy information publishers can generally limit their risk, for example, issuing acceptability guidelines to employees, or putting indemnity clauses into contracts with the freelancers who contribute columns. Software filtering technologies, which usually depend on searching for and blocking certain notorious sites by their address, or sites containing certain key-words or images, can be helpful to ISPs which seek to block access to

criminal content such as child pornography images, or particularly offensive words but are of little or no use at all in relation to fields like copyright (and libel).

Furthermore the content ISPs handle is in the main supplied by persons out of the control of the ISP, whereas a conventional publisher such as a newspaper can limit its risk, for example, issuing acceptability guidelines to its employees, or putting indemnity clauses into contracts with the freelancers who contribute columns. Software filtering technologies, which usually depend on searching for and blocking certain notorious sites by their address, or sites containing certain key-words or images, can be helpful to ISPs which seek to block access to content such as child pornography images, or particular offensive words, but are of little or no use at all in relation to content in breach of copyright (or other categories such as libel and hate speech). The ISP industry complained that if they were made to take responsibility for manually checking every item of content they carried, they would be unable to fulfil this duty due to the volume of traffic[31] and, faced with unquantifiable risk, would either go out of business, leave the jurisdiction for one with less restrictive laws, or be forced to pass the potential insurance costs on to the consumer, thus raising the costs of Internet access.

From the early 1990s therefore, in the US, the UK, and elsewhere, ISPs made vigorous claims that they should be exempted from liability on the basis of some kind of *innocent dissemination* defense - essentially claiming that had no effective control over the material they re-distributed, and thus should not be held legally liable in respect of it as publishers. To some extent this argument rested on whether ISPs were seen as more akin to conventional hard copy publishers, or TV and radio broadcasters - who have control over what they publish, and a corresponding duty to check that the material they publish is *not* defamatory - or whether they should be seen as more like "common carriers" such as the phone companies - who are seen as "mere passive conduits" for information, with no effective control over it, and who are thus usually not held liable for whatever material they carry. Somewhere between the two a third analogy or metaphor can be drawn, to newsstands or bookstores - persons who are responsible for distributing large quantities of potentially defamatory material and have some chance to examine it, but who cannot reasonably be expected to check it all in detail if they are to stay in business.

Two widely discussed early US libel liability cases failed to settle for US law the issue of whether

[31] The UK industry association, the ISPA, continue to protest this vociferously: see www.ispa.org.uk/html/media/content_liability.html, "It is not possible or practical for an ISP to monitor the content held on their servers because… ISPs deal with a vast amount of articles." They also cite the dynamic quality of Internet content, and how it can be "changed by the website owner in a matter of seconds".

ISPs should have the benefit of an innocent dissemination defense. In *Cubby v CompuServe*[32], CompuServe were sued in respect of an allegedly defamatory message appearing in a local forum hosted by them. CompuServe argued that they were merely a distributor of the information, not a publisher, and should therefore not be held liable. The New York District Court agreed, holding that CompuServe was here acting in a way akin to a newsstand, book store or public library, and that to hold it to a higher standard of liability than these distributors, would place undue restrictions on the free flow of electronic information. But in *Stratton Oakmont Inc v Prodigy Services*[33], on very similar facts, Prodigy was sued in respect of comments posted to a local discussion forum it hosted. The crucial difference from the CompuServe case (such as there was) was that Prodigy had explicitly marketed itself as "a family oriented computer network", which as part of its "value added" services, would control and prevent the publication of inappropriate messages. This seems to have been enough to lead the court to regard Prodigy as the publisher of the libels in question, rather than as a mere distributor, and accordingly they were held liable[34].? The most unfortunate aspect of the *Prodigy* and *CompuServe* decisions was that the ratio that could most easily be extracted from the two contrasting results was that to avoid liability, an ISP should do as little as possible to monitor and edit the content of the messages or other material it carries. This, it was argued, would make it seem more like a newsstand, and less like a publisher. But such a legal result (which can be labelled the "put your head in the sand" approach) was seen as having unfortunate results both for ISPs and the public interest in the development of the Internet.

As noted above, ISPs are seen as the natural gatekeepers to the Internet and are unarguably in the best position to filter out and stop the distribution of illegal and offensive content throughout the Internet. However public access to the Internet is predicated on a healthy, cheap and competitive ISP market, which placing unreasonable burdens on ISPs will not foster (especially as, compared to most industries, it is not that difficult for ISPs physically to relocate to a more permissive jurisdiction). So in the mid 1990s the debate centred on how best to encourage ISPs to take up an active role in the control of Internet content without reducing their business efficiency. There was a general consensus during the time of the "dot.com" bubble that market forces – the desire to gain and retain market share in a competitive market for Internet services - would lead ISPs, left to their own devices, to naturally take on an editorial and filtering role. The most obvious example of this related to spam. ISPs which deliver large amounts of unfiltered spam to its clients are unpopular and rapidly lose market share; hence ISPs have taken the leading role both in prosecuting spammers and

[32] 766 F Supp 135 (SD NY 1991).
[33] 1995 NY Misc. 23 Media L. Rep. 1794.
[34] *Prodigy* was in fact overruled by the US Supreme Court in a subsequent case, *Lunney v Prodigy Services Co*, on 5 February 2000 (available at http://www.courts.state.ny.us/ctapps/decisions/164opn.htm). However by that time, as discussed below, the force of the decision had been overtaken by the immunity provisions for ISPs introduced in the Communications Decency Act 1996. The case does however confirm that in US law an ISP is now officially regarded as not a publisher at common law.

developing anti-spam technology. Thus the task of legislatures, it seemed, was to *protect* or *immunize* ISPs from the liability they incurred under *Prodigy* law as content hosts or transmitters if they took a supervisory, filtering or monitoring role. In particular, legislatures should refrain from imposing technically impossible demands on hosts and ISPs that they monitor all traffic they carried or all content they hosted. This chain of thought led, as we shall see, to the legislative "safe harbor" or total immunity for ISPs and other online intermediaries provided in the USA by the Communications Decency Act 1996.

The rise and fall of intermediary immunities? After the dot-com bubble and the P2P wars

The self-regulatory surmise that ISPs, left to their own devices, would be prompted by the market to adopt a filtering and monitoring strategy, does not seem to have entirely transpired in the post dot.com bubble 2000s or, at least not on a consistent basis. For every BT Internet[35] and AOL who decide that it is a positive market strategy to be seen to try to remove and block access to child pornography or other illicit content, there are many others who see no advantage in holding themselves out, on the one hand, as censors or, on the other, as warehousers or distributors of obscene or illegal content. As the Oxford PCMLP research suggests[36], most ISPs would far rather be seen as anonymous middle-men and consider a filtering, monitoring and adjudicatory role as merely an extra cost and an activity which is peripheral and diverts from their core business. This suggests that if the public interest lies with online intermediaries taking a hands-on role in relation to illicit content, total immunity may not be the way to achieve it.

Turning to the particular issue of intermediaries and copyright material, the difficulty lies in balancing the interests of those authors and rightsholders whose rights are infringed with the argued need of intermediaries to be protected from liability. Some institutional owners of intellectual property rights – principally the recording, film, software and publishing industries – have argued strongly that ISPs must take some responsibility for the exponential growth in infringing material on the Net. Authors also have a moral entitlement to take action against intermediary hosts who give access to the world to unauthorised copies of their works, even after they have been notified of the problem[37]. The IP industries argue that ISPs (particularly since the advent of broadband, which is the *sine qua non* for effective downloading of films and games) have constructive if not actual

[35] BT Internet recently become the first major ISP in the Western world to offer a service which claims to filter out all child pornographic material they are alerted to in advance See "BT to block access to child porn sites", http://www.out-law.com, 8 June 2004. BT subsequently announced that in the first three weeks of blocking they had already blocked 230,000 attempts to access child pornography sites; one wonders how effective this makes it as a marketing strategy.
[36] See further, infra n90.
[37] See eg, *Ellison v AOL*, 189 F. Supp. 2d 1051 (C.D. Calif. 2002).

knowledge that they are making money out of extensive illicit downloading[38] and should not be simply allowed to turn a blind eye on the grounds that they are only the "messenger" and not the actual promoter of unauthorised use, including piracy. It is well known that many hosted sites and newsgroups are warehouses for illegal copies of software and music files, or repositories from which P2P software can be downloaded. ISPs, on the other hand, point out that high bandwidth downloading on what tend to be fixed rate bandwidth connections creates losses rather profits for them[39].

A final factor which might point to retrenchment on intermediary immunity is that the online intermediary industry sector is now rather more established and also more mainstreamed than it was in the times which spawned the ECD and the DMCA. It no longer seems plausible that major intermediaries, portals, hosts and ISPs like Yahoo!, AOL, BT, Amazon or eBay, faced with the imposition of less limited liability, would give up doing business, or relocate, exercise regulatory arbitrage and do business exclusively from (say) Vanuatu. Even if they did, there are alternative Internet access and content providers in the market now; the growth in wireless Internet and Internet services via mobile phone providers is significant here. It may be time for the specific ISP industry, at least, to recognise (or be forced to recognise), like other industry sectors, that certain legal risks simply have to be accepted as part of the costs of doing business, and that their own business interests have to be balanced against the needs both of rightsholders and the public interest. Of course this is a somewhat sweeping statement, and not necessarily applicable to all Internet intermediaries in every role they play. Search engines, for example, are vital both to doing business on the Internet, to scholarship and creativity, and to digital access and freedom of expression; it seems crucial to put as few content-related burdens on them as possible. Future legislators and judges may need to consider whether omnibus and horizontal "intermediary service provider" regimes covering all types of intermediaries and all types of content are really the best way to proceed. A subtler, more industry-sectoral content-specific approach may be needed (although of course it will have the drawback of being less immediately clear and applicable to lay industry professionals and users). And as we shall see, when we come to P2P intermediaries (see below p 38 et seq.) the policy and legal factors behind claims to either liability or immunity are very different for them than those outlined thus far.

F. Legal regimes for regulating online intermediary liability

[38] Some commentators have estimated that up to 80% of ISP traffic is now used for P2P downloading. "P2P packets have been said to comprise up to 80 percent of some ISP traffic volumes, and these applications are essentially the only ones driving widespread residential broadband deployment." See http://www.boardwatch.com/techchannels/oss/.
[39] Ibid. But note that, *because* of extensive downloading by some customers, many consumer ISPs are moving to charging in bands by amount of data downloaded as opposed to "one pipe fits all" flat-rate pricing.

Global approaches to regulating online intermediaries can broadly be divided into three categories:

(i) the "*total liability approach*":

Broadly, as the name suggests, intermediaries are liable in the same way as primary content providers are for illegal or actionable content. In practice, what this tends to mean is that intermediaries are directly threatened with criminal sanctions unless they fulfil their role as gatekeeper, and keep undesirable content out of the national jurisdiction where they are located. In the context of copyright, a university (say) which was found to be hosting infringing MP3 files would be as liable in copyright as the student who placed them there, and have no defense by virtue of being an intermediary. Such an approach has, of course, been applied not to enforce the laws of copyright, but in the main in certain non-Western countries where the Internet may be seen as a conduit for dissemination of subversive, seditious and politically unsettling material and ISPs are encouraged forcibly to act as an arm of state censorship[40]. Reed notes, for example, that in China, a form of strict liability is imposed on ISPs who are enjoined *inter alia* to refrain from "*producing, posting or disseminating pernicious information that may jeopardise state security and disrupt social stability, contravene laws and regulations and spread superstition and obscenity*". However, in the West such an approach has usually been regarded as both practically unworkable, and dangerously likely to impede freedom of speech.

An interesting attempt at legislating to this effect took place in Australia, in the form of the early version of the Broadcasting Services Amendment (On Line Services) Act 1999, which, in very different form, eventually came into force on 1 January 2000[41]. This Act dealt only with offensive content, mainly pornography, but also violent content. The Act was largely seen as a political gesture indicating the Government's commitment to ridding Australia of largely foreign-originated Internet porn, rather than as a practical exercise, but its history is instructive. When originally introduced, the shape of the scheme was broadly that Australian ISPs were required either to *remove* "prohibited content"[42] if they physically hosted the offending material within Australia (by order of a "take-down" notice); or to *block access* to it if it was physically held abroad (by order of an "access-prevention" notice). The sanctions for failing to do so were draconian: a scale fine of A$27,500 per day was imposed for failure to meet these duties, accumulating on a daily basis. The requirements of access-prevention were, however, dropped[43] after evidence was produced both by the ISP community and computer scientists that it would be technically impossible for ISPs to fulfil these

[40] See Reed C. "Liability of Online Information Providers – Towards a Global Solution" (2003) 17 (3) Int Rev LCT 255 at n 4.
[41] See at http://scaleplus.law.gov.au/html/comact/10/6005/0/CM000060.htm.
[42] "Prohibited content" was that classified as Refused Classification (RC) or X by the National Classification Board.
[43] Instead, Australian ISPs merely had to offer approved filtering products to subscribers, which would be updated to exclude the URLs of proscribed reports as they were reported to the authorities. Notably, ISPs were not compelled to install "upstream" filtering on their own servers, nor to make sure their subscribers actually used the filters made available to them.

duties, as proscribed sites might *inter alia* change URL, change IP address, or be accessed via proxy servers. Furthermore if access-prevention was impossible, it was said, then take-down of domestic content was also largely futile. Internet content is extremely portable, and any domestic host served with a take-down notice could fairly easily transfer itself to a foreign site simply by signing on with a foreign ISP; which would then be equally accessible by the Australian public.

The Australian experience is interesting for demonstrating, first, that public opinion may not back the imposition of total liability on intermediaries, even where they are the only effective way to solve a content problem, mainly on grounds of interference with freedom of expression; and second, that strict liability requirements of access-prevention (rather than of take-down by hosts on notice – see below) are likely to be impossible to fulfil. However, technologies have improved since 2000, and this excuse may no longer be as convincing. In the *Yahoo!* case, the Court, presented with the defense that it was technically impossible for Yahoo! US (Yahoo Inc) to block access to its Nazi memorabilia auction pages to all persons from France, remitted the question of practicality to a technical subcommittee to investigate. They reported back that, in fact, Yahoo! had the capacity (already used to serve up adverts in the relevant language to users from whatever country of origin) to identify and thus block access to 90% of French citizens[44]. Accordingly, Yahoo! were instructed to block access.

(ii) the "*self regulation/total immunity*" approach:

This rests on the belief, already discussed, that ISPs left to their own devices will, for commercial reasons, naturally take on an editorial and filtering role, so long as they are given protection from the risk entailed in being seen as publishers, distributors or the like. To facilitate this self-regulatory approach then, ISPs must be guaranteed total immunity from liability in respect of content they carry – the "common carrier" ideal. The leading example of "total immunity" regulation in global legislation is the US regime introduced by the Communications Decency Act 1996 (CDA), discussed above[45]. The CDA's primary goal was to prohibit the publication of obscene or indecent speech in cyberspace wherever it might be known to be accessible by a minor child – unfortunately, given the inherently un-zoned nature of most of the Internet, this was everywhere it appeared. The Legislature took the view that the Act would only be enforceable if ISPs, in return for their co-operation in monitoring and filtering content, were granted the *quid pro quo* of absolute immunity as publishers, in

[44] See *LICRA et UEJF vs Yahoo! Inc and Yahoo France*, Tribunal de Grande Instance de Paris (Superior Court of Paris), 20/11/2000 at p.14, at <http://www.gigalaw.com/library/france-yahoo-2000-11-20-lapres.html>. Around 70% of users' country of origin could be established from IP address and the remaining 20% or so could be made up by asking users to fill in a form declaring country of origin. Some degree of evasion would always be possible however because of use of foreign ISPs, proxy servers and anoymising services.

[45] Singapore provides total immunity to intermediary service providers but only in relation to transmission and caching liability, not, crucially, hosting : see n 65 infra.

respect of civil, criminal and statutory liability for all content originated by a third party[46]. Effectively, the *Prodigy* case (discussed above) was being reversed by statute. These main provisions of the CDA were however later struck down by the US Supreme Court as being unreasonably in breach of the constitutional rights of freedom of speech of adults[47]. Meanwhile, however, the statutory "safe harbor" for ISPs remained in force, and has operated, as was held in the case of *Zeran v AOL*[48], to wholly suspend actions in common law (including actions for negligence and defamation) against ISPs for publishing material originated by another content provider[49].

What may be given short shrift in this paradigm is the protection of authors and copyright holders, including those seeking take-down of infringing works. Since intermediaries are totally protected from liability, they can ignore even reasonable demands for take down without fear and institutional inertia will encourage them to do so. CDA jurisprudence illustrates this point. In *Zeran*, for example, Mr Zeran was libelled by an anonymous prankster who posted a message to an AOL forum offering t-shirts for sale glorifying the infamous Oklahoma bomber, and giving Mr Zeran's real name and address as the contact for the sales. Mr Zeran then suffered extreme harassment from persons incensed at his apparent bad taste. He asked AOL to remove the posting but they refused. When he sued them as publishers of a libel, they relied on s. 230(c) and were accordingly exculpated. Total immunity had given them carte blanche to ignore the legitimate demands of victims.

Another significant US case is *Blumenthal v Drudge*[50]. AOL paid Drudge, a well known political hack, $36,000 a year to provide them with an online political gossip column. Blumenthal, a Clinton aide, sued AOL for publishing an item libelling him within Drudge's column. Although AOL clearly benefited from the content Drudge supplied in terms of audience capture, since the content was provided by a third party not AOL, they were immune from any suit. Since AOL gained profit from Drudge's willingness to recklessly defame others, this was a clearly unjust result.

Interestingly there has recently been some retrenchment in US case law against the high water mark of immunity achieved in *Zeran* and *Blumenthal*, but this has not so far reached the stage of a consistent reversal of the general "total immunity" granted by s. 230(c). In the US, a series of court cases such as *Barrett v Rosenthal*[51], and, most recently, *Grace v EBay*[52] have begun to successfully attack

---

[46] See. 230 (c) which provides "*No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another content provider*." See further judicial interpretation in *Zeran v America Online* 1997 US Dist Lexis 3429 (E.D. Va. Mar.21 1997) , *Blumenthal v Drudge* 1998 BNA EC&L 561.

[47] Supreme Court decision in *Reno v ACLU*, (1997) 2 BNA EPLR 664, available at http://www.aclu.org/court/renovacludec.html.

[48] 1997 US Dist Lexis 3429 (E.D. Va. Mar.21 1997).

[49] See also *Doe v America Online Inc*, Fla Cir.Ct, Palm Beach Cty, No.CL 97-631 AE, 13 June 1997.

[50] See n 46 supra.

[51] 114 Cal.App.4th 1379 (Cal. App. 1st Dist.), Cal. Sup. Ct., review granted.

the "total immunity" granted to online service providers by the CDA. It is clear that a number of US courts find the "total immunity" regime an unhelpful one, when considering the rights of third parties affected by the negligence of intermediaries. Although intermediary liability for copyright is controlled in the US by the DMCA and not the CDA, the point is relevant to construction of any global regime for regulating the immunity of copyright intermediaries.

So far we have seen that the "direct approach" is something of an unworkable solution and tends to be seen as an arm of state censorship, while the "total immunity" approach is open to abuse from ISPs and poor at protecting the interests of third party "victims", including authors and copyright holders. What then of the third, middle ground approach?

(iii) The "limitation of liability/notify and takedown" approach

This is currently the approach taken in a number of notable jurisdictions, for example the US DMCA and the ECD (Articles 12-15), as well as in other national laws such as the German Multimedia Act 1998 (Article 5) and the Japanese Law of 2001[53]. Roughly, the view is accepted that online intermediaries should be protected from the unlimited risk they are prone to as publishers, hosts and conduits, if they are to operate; but on the other hand it is recognised that total immunity can be abused and should be balanced against other policy factors, such as the need to protect holders of intellectual property rights.

The EC Electronic Commerce Directive (ECD)

The ECD takes a horizontal approach to the liability of information society service providers (ISSPs) – in other words it deals with all kinds of content issues, whether intellectual property, criminal obscenity, libel, *et al* – rather than focusing on a single area. Furthermore, rather than giving a blanket immunity to ISPs in *all* circumstances where the content is provided by a third party other than the ISP, as the US CDA s. 230(c) does, it takes a more subtle approach in which the various activities of ISPs are addressed separately. Where ISPs act as a "mere conduit" – ie, as a relay station transmitting content originated by and destined for other parties – the Directive, in the form of Article 12, regards them as basically absolved from all liability. To maintain immunity, the ISP must not initiate the transmission, select the receiver of the transmission or modify the information

---

[52] 2004 WL 1632047 (Cal. App. 2nd Dist. July 22). EBay were sued for defamatory remarks made on its auction site by a disgruntled bidder in respect of another user of the site. But note that although EBay lost on CDA immunity, having been found not to be a publisher of information but a distributor, they still were held not liable because their contractual terms successfully excluded liability. The message to ISP lawyers is clearly to review their subscriber terns and conditions and not rely on legislative immunities.

[53] Law No 137 of 2001. See Yamaguchi I. "Beyond de Facto Speech: Digital Transformation of Free Speech Theory in Japan" (2002) 38 (1) Stanford Journal of International Law 109 at 114.

contained in the transmission[54]. This is very much in line with the position as to liability for "common carriers" such as the post office and the phone company. The Directive also makes it clear[55] that ISPs will not be held liable simply because they *cache* material. Since the effect of caching is to speed up the Web for all users since traffic is reduced, it is important that caching not be legally discouraged lest the Internet slow to a crawl. As with the "mere conduit" provision, immunity is subject to the requirement that the information not be modified by the ISSP and also that the cached copy be updated regularly according to industry practice.

More controversially, immunity is also subject to the ISSP taking down cached copies once they obtain actual knowledge that the original source of the information has been removed or access to it disabled, or removal or blocking of access has been ordered by a competent court or authority. These provisions may be a serious concern for some hosts, notably search engines, who sometimes maintain copies of material locally to assist searchers even when they have moved on the original site, and mirror sites set up to reduce the demand on a single site offering popular pages[56].

The main controversy in the ECD regime has centred on the hosting provisions in Article 14, which deals with circumstances where ISPs host or store more than transiently content originated by third parties. One important point is that Article 14(2) provides that content is not to be treated as originating from a third party if that recipient acts "under the authority or control of the [ISSP]" – thus the ECD avoids the difficulties found in *Blumenthal* above, where Drudge would almost certainly have been found to be acting under the "authority" of AOL and hence AOL would not have benefited from immunity.

Under Article 14, ISSPs are declared exempt from liability in respect of the storage of information provided by a recipient of their services, so long as they have no "actual knowledge" of "illegal activity or information" (criminal liability); and, as regards claims for damages (civil liability) are immune as long as they have no such actual knowledge *and* are not aware of "facts and

---

[54] Article 12. Transmission includes automatic, intermediate, and transient storage. Presumably "information" excludes header information which ISPs routinely and automatically add to through traffic they forward. Such header information is vital to the routing of packets through the Internet to their destination, but does not form part of the message information actually read by the recipient.

[55] Article 13. Worries that the European Parliament had introduced provisions incompatible with Article 13 at the draft stage of another EC Directive, on copyright and related rights, were partially allayed by the final text.

[56] See further discussion on notice and take down in relation to Article 14 below. Immunity for caching is most obviously relevant to content copied by an ISP *prima facie* in breach of copyright. However it is conceivable that a cached copy of a page containing libellous or obscene material might be deemed to be "published" by an ISP or host since it can still be retrieved by other subscribers to that ISP seeking that particular page until the cache is purged. In the US, cease and desist letters under the DMCA demanding "take down" of material infringing the copyright of the rights-holder are now frequently being received by the search engine Google, which maintains cached copies for a short period of material even after it has been removed from the original host site. See, as sample, report of such request from Church of Scientology to Google at http://chillingeffects.org/dmca512/notice.cgi?NoticeID=1352 and request for removal of a "collection of recipes" at http://chillingeffects.org/dmca512/notice.cgi?NoticeID=1327.

circumstances from which the illegal activity or information is apparent". Although this implies that ISSPs may be liable in civil though not in criminal law for constructive as well as actual knowledge, it is made very clear that they do not have to go out and actively *seek* this awareness in Article 15. This provides that EC Member States are not to impose any general monitoring requirement on ISSPs, although ISSPs may be asked to inform the authorities of allegedly illegal activities they do happen to come across. In practice, the main debate around Articles 14 and 15 has concerned not constructive knowledge but *actual* knowledge, and its implications in the forms of "notice and take down". These are discussed in detail below.

The DMCA and linking liability

Section 512 of the US DMCA introduced a similar scheme of immunities, or as they are known, "safe harbors" – transmission[57], caching[58] and hosting[59] immunities - to the ECD but in relation to intermediary liability for content infringing *copyright only*, ie, it is a vertical not horizontal provision. The notice and takedown regime for hosts ushered in by the DMCA in s. 512(c) is considerably more detailed than that in the ECD[60], and has generally been greeted with more enthusiasm both by rights-holder groups and ISPs for reasons discussed below. An issue expressly dealt with by the DMCA but left out the ECD is the question of *linking liability*. This is a particularly crucial matter to consider for search engines sites, which as their raison d'etre create links to unknown material. "Hosting" as dealt with in Article 14 of the ECD requires the undefined word "*storage*", which seems to imply that merely making a hyper-link to content cannot constitute "hosting" - therefore any liability which *may* arise in relation to a hyper-link under a European national law is *not* excluded by Article 14. The DMCA by contrast expressly grants immunity[61] to "information location tools" pointing to infringing material under certain conditions. The European Commission is specifically instructed to review this matter for the ECD on an ongoing basis by Article 21(2) of the ECD. So far, Spain, Austria, Lichtenstein and Portugal have all chosen to extend intermediary immunities to cover linking liability, while all other states have so far not, creating a perhaps unhelpful cross-Europe disharmony.

Linking is of ever greater significance as the Internet becomes manageable only via search engines

[57] Section 512(a) – Transitory Digital Network Communications.
[58] Section 512(b) – System caching.
[59] Section 512(c) - Information Residing on Systems or Networks at Direction of Users. It is notable compared to the CDA and *Blumenthal v Drudge*, that intermediary ("service provider") immunity for hosting is dependent on the service provider not receiving a financial benefit from the infringing activity where it has the right and ability to control such activity.. 512(c)(1)(B).
[60] This might be seen as inevitable given that EC Directives are only supposed to provide a framework for national implementation. However, as discussed below, the problem has been (i) that many EU Members have simply implemented the words of Article 14 without adding national detail to the notice and take-down (NTD) provisions (ii) that as a result it cannot be guaranteed that NTD will be harmonised in any detail across Europe.
[61] Section 512(d), Information Location Tools.

and, as noted above, these are already becoming the frequent target of cease and desist letters and thus must be uncomfortably conscious of their position of globally uncertain legal immunity. Since the drafting of the ECD, aggregators have also become important intermediaries – sites which provide links to a variety of sites so that, say, a user can read the headlines from multiple news sites conveniently on one page. Such aggregators are technically making links to a wide variety of "upstream" content over which they may or may not have technical control to remove individual items, depending on how their software code is implemented[62]. Similarly price comparison sites generate links to a wide variety of sites ranked by factors such as price and availability and are an important feature for the Internet in promoting consumer choice. It may be desirable, both for reduction of business risk to portal etc sites, and harmony with the US DMCA scheme, that immunity from linking liability be taken into consideration for adoption by other jurisdictions in the future.

This may however be a controversial step in Europe. In Germany recently, as in France during the *Yahoo!* case, ISPs have been successfully ordered to block access to sites abroad and at home offering access to hate speech[63]. This is a trend which can be discerned across Continental Europe, where states are perturbed to find that their post-WW II anti-Nazi laws forbidding glorification of Fascist and racist speech are being overwhelmed by a deluge of hate speech content stored, legally, on US servers[64]. They then have no way to attack the phenomenon except by demanding that local ISPs block access. A copyright-only statute, of course, can claim not to be concerned with matters of hate speech and obscenity; however this fits poorly with the horizontal structure of the ECD and other jurisdictions with horizontal immunity statutes, such as Singapore.[65]

---

[62] As an example, Lawrence Lessig, the well known cyber-lawyer, maintains a popular weblog site at http://www.lessig.org/blog/. The site can be accessed directly via the Web but it can also be delivered as an "RSS feed" to other sites, ie, as text in XML form, which can be aggregated by any other content providing site. Thus, this writer can say, read Lessig's blog along with Eugene Volokh's blog, several friends' blogs, and sundry news headlines all on one page at (say) http://www.livejournal.com, a blogging site, as her start to the day. Suppose Lessig declares (untruthfully) that all of Edwards's work is plagiarised from her students on his blog. I demand that LiveJournal.com remove the item from their RSS feed delivered to many other thousands of users who read the Lessig blog via LiveJournal. LiveJournal's technical ability to do so depends on the format of the original XML text supplied. Although it will normally be possible to remove a single item, as a worst case scenario, it might conceivably not be possible for them to take down the alleged libellous item without disabling the entire feed. The administrative overhead of such take-down for aggregators, who often offer this service for free, will also be not inconsiderable.

[63] See Schumacher P. H. "Fighting Illegal Content – May Access Providers be Required to Ban Foreign Websites? A recent German approach" (2004) 8 Int J Comm Law and Policy available at http://www.ijclp.org/8_2004/pdf/schumacher-paper-ijclp.pdf . The German Teleservices Act 1997, article 5(4) specifically provides that even though access providers are provided with blanket immunity, this falls if they know the material they provide access to is unlawful and fail to comply with a legal duty to block access.

[64] Ryan N. "Fear and Loathing", *The Guardian,* Online Section, Aug 12 2004, at http://www.guardian.co.uk/online/story/0,3605,1280992,00.html.

[65]Singapore Electronic Transactions Act 1998 provides in s. 10(1) that : "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." Section 10(2) adds that "For the purposes of this section - "*provides access*", in relation to third-party material, means the provision of the

Finally, it might be briefly noted that much of the debate around the liability (or not) of P2P sites post-*Napster* has been over whether liability can be ascribed to intermediaries who are not hosting illicit content but, in essence, merely pointing others towards it, albeit sometimes at several removes. This is, effectively, still, what Grokster supernodes and BitTorrent torrent aggregator and "tracker" sites are doing. Indeed, one UK based BT pirate "hub" (torrent aggregator site) has recently announced that they intend to fight a cease and desist notice from the MPA on the basis that they are fulfilling the same role as a search engine[66]. Does "pointing towards" equate to "linking" and if so, should immunities for linking potentially also protect some P2P intermediaries which find themselves open to challenge and liability on the *Napster* principle? As noted in more detail below[67], *Aimster*'s defence that they were an "information location tool" under s. 512 (d) of the DMCA has already been rejected by the US courts, as was Napster's own claim that it was merely transmitting information under s. 512(a), the equivalent of the ECD's "mere conduit". (*Grokster* of course did not need to avail themselves of a "safe harbor" defense, and such would in any case not have been appropriate to its architecture.) Other jurisdictions however may yet take a different approach and be more ready to equate P2P intermediaries with link and access-providers as deserving of immunity.

A recent Belgian ISP case may be the first European case to raise this point. The IFPI, the international representative of the recording industry, has instigated legal proceedings against the Belgian ISP Telenet for the unauthorised distribution of music via Usenet (newsgroups)[68]. Telenet refuses to block the access to certain newsgroups in its newsservice "Bommanews" which are known to be used for distributing illegal music files. The ISP argues that providing Usenet services is a "mere conduit" activity, and under the E-Commerce Directive a provider cannot be held liable for just passing bits. If ISPs cannot be held liable for giving access to infringing MP3s under the ECD immunity clauses, then can such reasoning not also apply to the likes of Napster and even more so, KaZaA and BitTorrent? Interestingly the Belgian ISPA while supporting Telenet - "As ISPs we don't initiate the transmission, we don't select the recipients, and we also don't select or modify the newsgroup content which is being transmitted". – is actually seeking settlement outside the Court, with its preferred outcome a soft-law Protocol that would describe how the regulatory authorities,

---

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." Arguably this is wide enough to cover provision of access by hyperlinking; however as it does not even seem to extend to permanent storage/hosting (as opposed to caching), this was probably not the legislative intention.

[66] See "Hollywood threatens to sue UK BitTorrent man for millions" *The Register*, 15 March 2005, at http://www.theregister.co.uk/2005/03/15/mpaa_hanff_suit/. " 'Torrent files don't contain any data," Hanff said. "This is a search engine scenario. Why aren't Google, Yahoo or Microsoft getting sued?'"

[67] Infra page 44.

[68] EDRI-gram - Number 2.3, 11 February 2004 "IFPI sues Belgian ISP over Usenet", 11 February 2004.

copyright holders and ISPs would handle future manifestations of infringing content in newsgroups.

G. Hosting, notice and takedown: the self regulation conundrum

Limited liability regimes such as the ECD, DMCA and German Teleservices Act limit immunity mainly by the means of "notice and takedown" (NTD) procedures. Intermediaries are typically protected from liability up till the point where they gain actual or constructive knowledge that such illegal content exists, at which point they come under a duty to block access to or take down the content. This raises various problems.

Expedience

What if an online intermediary is notified by a rightsholder that a Web site the intermediary hosts contains unauthorized copies of material belonging to the rightsholder and can it be taken down immediately? Does the intermediary become liable straight away since they now have actual "knowledge" or "awareness" that the content may be illegal? Article 14(1)(b) of the ECD provides specifically that so long as the ISP "*acts expeditiously to remove or to disable access to the information*", they will retain their protection from liability, even after notice. No guidance is given in the Directive as to what *"expeditiously"* means, however, and whether it allows enough time to, for example, consult an in house lawyer, find an external lawyer or request counsel's opinion. In large ISPs, it may take some time for a take-down request to find the appropriate employee, while in small ISPs, it may be difficult to identify an employee with the resources to take charge of the request; and how these indoor management issues affect "expedience" remains unclear. Article 14, furthermore, seems to imply that once notice has been given and the expedient period of grace expired, liability is strict even if take-down presents technical or administrative problems. The DMCA also requires that the service provider act "*expeditiously to remove or disable access to the material*[69]".

A better alternative might be, as the German Multimedia Act and indeed the Australian legislation discussed above provided, for liability to arise only after the ISP has failed to take some kind of "reasonable steps" ie, a duty of care rather than strict liability. This problem of whether mere fulfillment of a reasonable level of duty or actual removal/blocking of content should be demanded, is exacerbated when we talk of access-prevention, which is intrinsically less controllable by the intermediary than hosted content-removal (cf the *Yahoo*! Case, where as we have seen, the Parisian court investigated thoroughly the practicality of the order for access-prevention they made), but it is also relevant to ordinary hosting liability.

[69] Section 512(c)(1)(A)(iii).

NTD, free speech and privatized censorship

This is the main source of controversy around NTD. In the UK, a debate was sparked by the case of *Godfrey v Demon Internet*[70], a libel liability decision which preceded implementation of the ECD but was dealt with under a similar set of rules in s. 1 of the UK Defamation Act 1996. The case involved allegations by a British physicist, Lawrence Godfrey, that an anonymous hoax message posted in a newsgroup, soc.culture.thai, in 1997, was libelous and damaging to his reputation. Godfrey asked the ISP Demon, who carried the newsgroup in question, to remove the offensive posting. When Demon did not comply, Godfrey raised an action against them for publishing a libel. Demon claimed the benefit of the s. 1 defence under the Defamation Act 1996, which provided in substance, much as Article 14 of the ECD does now, that an ISP could claim immunity as a host so long as it could claim that it "*did not know and had no reason to believe what [it] did contributed to the publication of a defamatory statement*".[71] Because Demon *had* been notified of the allegedly libellous posting and not removed it, the judge held that they clearly fell foul of s. 1(1)(c) and thus could not take advantage of the s. 1 immunity.[72]

The message forcibly sent by *Godfrey* to ISPs was thus that, in the interest of avoiding litigation, they would be best served by removing or blocking access to any item of content hosted by them which was brought to their notice without too much fuss, however unfounded or trivial the objection might seem to be. Cyber-liberty groups protested that this had serious implications for freedom of expression since in effect, any crank caller or pressure group could now censor text posted on the Internet simply by complaining that it was illegal to the ISP. Intermediaries might thus be forced into taking part in what has been termed "privatised censorship" even though they do not have the constitutional authority or legal knowledge of a court or lawyer, nor, in general, the desire to take on the role of a court. (Small or free ISPs or host sites may not even have anyone on staff who is legally qualified, or even if so, still may not be knowledgeable in the niceties of Internet law, libel, copyright, privacy and obscenity law[73].)

One constraining factor on an intermediary's willingness to take down might be that if access to a Web site is removed as containing illegal material, but it is later exculpated in court, the intermediary

[70] [1999] 4 All ER 342, [2000] 2 WLR 1020.
[71] 1996 Act, s. 1(1)(c).
[72] The case was subsequently settled.
[73] See discussion in Ahlert C. Marsden C. and Yung C. "How Liberty Disappeared from Cyberspace: the Mystery Shopper Tests Internet Content Self-Regulation" ("*Mystery Shopper*"). In a survey of Dutch ISPs, out of five who responded, none said they would involve a lawyer in examining take down requests. The overall impression given is that ISPs regarded dealing with take down requests as a time sink which did not contribute to their core business goals.

might conceivably suffer a breach of contract claim from the content provider whose material was taken down. In this worst case scenario, an intermediary might fairly consider itself hard done by: damned if it does take down and damned if it doesn't. Under the DMCA s. 512(g), when an ISP "takes down" on request of a rights-holder in good faith it benefits from a safe harbor which protects it from any liability arising from that takedown. No such equivalent protection exists in the ECD (although as the Directive is a minimum harmonisation there is no reason EC Member States cannot introduce such). It seems likely from anecdotal evidence, though, that ISPs in any case regard the easiest way out of a difficult situation is to take down first and hope not to be in breach of contract second. Well drafted terms of the subscriber contract can probably control the latter risk, and ISPs serving consumers may also rely on the inertia of consumers in relation to litigation, while the former risk of being held liable for illegal material not removed expeditiously is one which cannot easily be avoided by private mechanisms[74] and may attract the attention of efficient public or industry law enforcement authorities where obscenity and copyright infringement are concerned. Empirical research conducted by Oxford researchers for the EU into the mechanism of notice and take down in the ISP industry concluded in 2004 that "*the current regulatory settlement has created an environment in which the incentive to take down content from the Internet is higher than the potential costs of not taking it down*."[75]

It is useful to take the *Godfrey* case and change the facts to a copyright scenario. What if the Godfrey was complaining that Demon were hosting a pirate copy of a textbook he had written? This seems a simple NTD scenario, but consider what duty if any would the ISSP come under either to check the facts, or consider the law relating to any potential defense, such as fair comment, educational use or private non-commercial copying (a defense in many Continental systems)? Would they, in practice, be likely to engage in any checks at all? As already noted, the time available for verification for an ISSP is already likely to be limited given the vagueness of the term "expediently". In practice, there is often little incentive for an ISP to do any investigation at all. In research carried out at Oxford known as the "Mystery Shopper" test, a major UK ISP was asked to take down a web page which was alleged to be a pirate copy which infringed copyright belonging to the complaining rights-holder. In fact the Web page contained Chapter II of John Stuart Mill's "On Liberty" which was published in 1869 and had long been in the public domain. Nonetheless the webpage was removed

[74] In fact to some extent it can be: this writer has earlier recommended (see Edwards "Defamation and the Internet", 2000, supra n 3) that ISPs could take out liability insurance against potential risk, as other commercial operations do when specific legal challenges about their activities are brought to their attention; or could insert into contracts with their own subscribers clauses which require such subscribers to indemnify them if the ISP subsequently incurs legal liability as a result of content originated by that subscriber. However it seems that the market has not developed support for either suggestion. See *Rightswatch* report conducted by the MCPS-PRS Alliance, on behalf of the European Community, November 2002-January 2003 (www.Rightswatch.com), section 9.10 (on insurance) and 9.2 (on indemnities). Consumer indemnity clauses might also be challengeable as unfair under European and UK consumer protection legislation such as the EC Unfair Terms Directive and the Unfair Contract Terms Directive 1977.

[75] *Mystery Shopper*, supra n 73, at 12.

without demur[76]. A major US ISP was also asked to remove the text, and instead of immediately so doing, sent a standard DMCA response requesting proof that the correspondent was the proper person to make such request (see below) and a statement of good faith. The Oxford team took this as evidence that the DMCA scheme was more likely to spur investigation than the UK NTD regime (such as it is); in fact, however it would not have been hard also to fake these credentials and there was no evidence that, crucially, the public domain status of the text would have been queried, rather than the identity of the rightsholder. As noted above, ascertaining take-down is formally correct is important to intermediaries under the DMCA as it protects them from action for breach of contract by maintaining their good faith "safe harbor" status.

Similar research was carried out subsequently by Sjoera Nas at Bits of Freedom, a digital human rights group based in the Netherlands. Nas, posing as copyright owner and complainant, asked 10 Dutch ISPs to remove works by Multatuli, a Dutch writer who died in 1860 and hence was in the public domain. Seven providers took down the text without apparently checking it out at all; one failed to respond to the complaint; one examined the text complained of and noted it was in the public domain (xs4all, a small ISP with a history of digital rights activism) and one forwarded the complaint to the website owner. Her "takedown hit rate" was thus 70%. [77]

It is extremely difficult to find evidence to rebut these worrying findings, as it is hard to gather information, positive or negative, on how ISPs or other intermediaries deal with NTD. Surveys of ISP behaviour in this field have in general notoriously low response rates; even one carried out by the UK ISPA, the industry's own local trade organisation, had so low a response rate that no statistical analysis was ever issued[78]. As noted above, intermediaries have little to gain from cooperating with research in this area: if they admit to taking down with alacrity, they look like censors (and possibly negligent ones at that); if they don't, they run the risk of incurring liability under provisions like the ECD. In public relations terms, there is little to gain from sticking up publicly for those who own or distribute porn, libels, or even, perhaps, infringing MP3s and movies. The key point perhaps is that online intermediaries largely have no perception of playing a public role – they are, bar a few exceptions like xs4all, private organisations driven by their profit margins - and unlike the traditional media sectors, have no fundamental stake in protecting freedom of speech.

Authorisation, detail and put-back

[76] See "*Mystery Shopper*", supra n 73.
[77] See further http://www.bof.nl/docs/researchpaperSANE.pdf.
[78] The UK ISPA commissioned a survey of ISPs which was reported in the UK press in December 2002, but not otherwise published; informal enquiries by Edwards established it had a very low return rate and was thus of dubious methodological value. The research did cover all types of Internet content and concluded that European ISPs were "overwhelmed" with requests for "takedown" and wanted to avoid "playing the role of judge and jury".

Another issue around notice and take-down relates to what authority should be needed to request take down. The DMCA requires (s. 512(c)(3)) that notice must be given in writing, and a physical or electronic signature of the person showing authorization to act on behalf of the rightsholder provided. By contrast in the UK *Godfrey* case, Demon's lawyer complained to the press that this meant he would have to take down every time he received a request from anybody, written in crayon on the back of an envelope. The DMCA further requires that the service provider provides a designated agent to whom takedown requests can be directed, and that details of exactly what infringing material is to be taken down, and where exactly it is held, should be supplied. By contrast the ECD is entirely unprescriptive on all these points.

The most important detail of a NTD scheme is how, or indeed, if, content providers should be given an opportunity to defend themselves before intermediaries block access to or take down content. Nothing in the EC regime even requires notification to the site whose content is taken down, and largely this would be a matter for each ISP's contractual rules and internal procedures. The requirement of "expedient" take-down of course again encourages an ISP even further to take down now, and notify later, if at all. Yet arguably until content has been proven illegal by a court or at least authoritatively labelled as such by a relevantly authorised professional such as a prosecutor (the approach taken in the Belgian implementation of the ECD) it should remain in place, otherwise administrative prior restraint is effectively operating to "chill" freedom of speech and restrict the reasonable contractual expectations of content providers. The DMCA provides that a take-down notice *must* be notified to the "owner" of the material which is to be taken down, who then has the opportunity to intervene and protest that the material should not be removed ("counter-notification")[79]. If that person disputes that there is copyright infringement then the material in question is "put back" by the ISP. If the original notifier then continues to dispute the legality of the content, the argument can be moved fairly rapidly into the courts and away from the "privatised" non-judicial control of ISPs. While dispute is under way, the ISP is given "safe harbor" to keep the content up, free from liability even if in the end a court does decide the content was illicit or actionable. Put-back is in principle an excellent device and a useful defense to the charge that NTD schemes impose covert private censorship aided and abetted by intermediary inertia. Yet the anecdotal evidence from the USA[80] is that few content providers threatened with cease and desist

[79] Section 512(g)(3).

[80] See especially the "Chilling Effects Clearinghouse" at http://www.chillingeffects.org, a joint project of the Electronic Frontier Foundation and Harvard, Stanford, Berkeley, University of San Francisco, University of Maine, and George Washington School of Law clinics, which gives notice to the public of "cease and desist" take-down letters received by a wide variety of hosts including, notably, the search engine Google. It is also useful to look at Creative Commons who operate inter alia at http://www.creativecommons.org in the USA and at http://creativecommons.org/projects/international/uk/in the UK.

letters do hold out for put-back let alone legal action even where facts in the cease and desist letter are false, or defenses could be mounted[81]. There are clear incentives for such behaviour: the desire for a quiet life, consumer inertia, fear of official letters. And of course, in the domain of unauthorised music and movies, settlements for damages imposed by the RIAA on illegal downloaders who co-operate, are generally much lower than the potential court-imposed fines or damages and costs of legal defense.

A role for public scrutiny of NTD?

Is there an institutional role for a body to act as a middle man between rightsholder and intermediaries? In the area of child pornography[82], a non-governmental "quango", the Internet Watch Foundation[83], has existed in the UK since 1996 to provide a means by which the ISP industry as a whole can receive notice and directions as to whether allegedly illegal content complained about by the public should be taken down. The IWF provides a free hot-line channel and a website, so that the public can report offensive material by phone, email or fax. An IWF model, it can be argued, is good for the public interest since it means take down requests will be scrutinised rather than possibly simply complied with by individual intermediaries lacking time and/or legal resources; and IWF decision making is also to some small extent transparent, as statistics are issued about types of complaints and action taken. By contrast the Oxford research[84] clearly seems to suggest that individual ISPs when considering complaints may be neither accountable, transparent nor necessarily applying the relevant legal rules.

This experience begs the question whether take-down requests by IP rights-holders might usefully also be funneled via a single institutional body (other than the courts, of course) which would then be in a position to exert considerable influence over ISPs and hosts in relation to take-down of alleged pirate material, just as the IWF does in relation to obscene material? This was one of the initial suggestions considered by the Rightswatch project funded by the EC from 2002-2003. In the end, however, the project members could not reach agreement on what the role of such an institution would be: whether it should merely act as a "postbox", should investigate and validate complaints, or should actively search for hosted pirate material. Most significantly, the Rightswatch project revealed substantial lack of consensus between the interests of the various stakeholders in the market. Four stakeholder groups were identified: ISPs, rights-holders, content providers and

[81] Wendy Seltzer of the EFF produces convincing evidence that many DMCA C&D letters do contain errors of fact and law: see http://www.eff.org/IP/P2P/20030926_unsafe_harbors.php .
[82] Although it has recently also begun to scrutinize racist and hate speech material.
[83] See http://www.iwf.org.uk.
[84] See "Mystery Shopper", supra n 73.

"users" or the public. "Trusted" major rights-holders such as music companies had their own legal staff and procedures in place and saw no advantage in a mediating third party. Smaller "non-trusted" rights-holders feared that they would be given less rights and less hearing than major rights-holders in an institutional scheme. The ISP sector's main concern was not for improved validation of the legal substance of take-down requests – indeed their overwhelming wish was to avoid making difficult, time consuming, unpopular and costly[85] decisions about takedown - but for a legally enforceable safe harbour to protect them from suit if and when they responded to take-down notices. For them, a new self-regulatory scheme involving a copyright "IWF" had little improvement to offer over the current status quo. "High levels of mutual hostility" were, furthermore, identified between ISPs and rights-holders. Groups representing content providers and users were mainly concerned with citizen access to information and freedom of speech issues, and felt they had no real involvement and representation in the current process. For them, there was a "*strong view that civil liberties are being replaced by consumer rights and judicial due process is being replaced by industry self regulation*".[86] The Rightswatch project thus produced no clear way forward, and is a strong indication of the obstacles to agreement among stakeholders on voluntary NTD regimes, absent statutory underpinnings.

It might usefully be asked what is desired – *post* publication removal or blocking of Internet content only on the demand of a properly empowered institution or court, thus respecting all legal defenses and the public interest; or some degree of cheap speedy restraint on illicit Internet content by the operation of NTD. If we want the latter, can we introduce an element of public scrutiny more effective than the put-back rules of the DMCA? The issue here is really what body (if any) should adjudicate on notice and takedown - judicial or administrative, self-regulatory or with a more public constitutionalised role, industry funded or state funded, open or acting behind closed doors. The IWF, for example, clearly provides effective scrutiny of a sort, and performs a quasi-public role, yet it is not a court or tribunal and has a self-appointed membership not consisting of lawyers or judges, but largely drawn from the ISP industry, law enforcement and children's charities. Content providers whose material is taken down have no *locus standi* to argue their case before the IWF. Natural justice might suggest a need to consider democratic appointment rules and participation rights for content providers[87]. Other models somewhere between NTD and a full court hearing are possible. In Belgium, take down of content by an ISP must be authorized not by a full court but by a state

[85] The UK ISPA's research in 2002 suggested that every take-down notice costs an ISP up to £1000 to process. See "ISP Liability Update: notice and take down" (2003) *Electronic Business Law* (April) 16.
[86] Rightswatch Final Report at para 5.5.
[87] Intermediaries of course can provide alternative dispute resolutions themselves to deal with such complaints, and since the passing of the Communications Act 2003, UK ISPs are in fact under an obligation to provide access to an external dispute resolution scheme to deal with customer complaints. Aggrieved ISP customers can go to Otelo, the Office of the Telecommunications Ombudsman, or to CISAS, an approved scheme backed by the ISP industry.

prosecutor.[88] In Italy and Spain, ECD-based regulations demand that "a competent body" determine the legality of disputed content. In the UK, the Publisher's Association, have proposed a scheme whereby as soon as "take-down" is opposed by the provider of the disputed content, the matter must mandatorily go to the courts and the content meanwhile remain in the public view[89].
What the "Mystery Shopper" and associated Oxford research, as well as the US experience recounted on the "Chilling Effects" site, seem to establish is that the interests of legal control of content, freedom of speech and natural justice may not be best met by leaving take down entirely to the control of the online intermediary industries. The Oxford PCMLP-IAPCODE[90] research identifies a number of essential requirements for a self regulatory dispute resolution system to work effectively and in the public interest in the digital media/content area. Such schemes should be, inter alia:

- Beneficial to consumers;
- Accessible to members of the public;
- Independent from interference by interested parties;
- Adequately funded and staffed;
- Provide effective and credible sanctions;
- Provide for auditing and review by the relevant independent regulatory authority (IRA);
- Be publicly accountable; and
- Provide for an independent appeals mechanism.[91]

It seems evident that existing bodies making decisions on take-down, such as ISPs, hosts and even self-appointed institutions like the IWF, do not currently meet most or all of these criteria[92]. The Oxford research suggests[93] that the way forward may lie with codes of conduct developed by relevant industry bodies accredited by the relevant IRA (Independent Regulatory Authority) for that industry sector. This provides both flexibility and public input into NTD practice. Accreditation could be indicated by kite marking. The IRA should also then continue to audit such self regulatory schemes in some co-regulatory paradigm, in order to assess how they are impacting fundamental rights such as freedom of speech, via a "Fundamental Rights Impact Assessment". A "national

[88] Recent Canadian proposals recommend a 'notice and notice' procedure which would require a court order prior to the removal of content. See Geist. M "Canada rejects one-sided approach to copyright reform", Toronto Star, March 28, 2005.
[89] Oral presentation by PA representative, *Not-Con*, London, 5 June 2004.
[90] Oxford PCMLP-IAPCODE "Self regulation of digital media converging onto the Internet: Industry codes of conduct in sectoral analysis" available at http://pcmlp.socleg.ox.ac.uk/execsummary.pdf
[91] PMCLP-IAPCODE, ibid, para 12.1.
[92] Oddly, the much criticized Australian scheme discussed infra does in fact involve public scrutiny by a legitimate government appointed body, namely the ABA Classification Board. It also publishes full reports of its activities.
[93] Ibid, Section 12: Watching the Watchdogs: Accreditation of Self-regulatory Codes and Institutions.

resource audit of ISP and content sectors" should also be undertaken to see if ISPs have the resources sustainably to devote to effective self regulation. Structures should be assessed to see if and how they incorporate independent representation, external monitoring of compliance, public accountability and adequate publicity and transparency functions. Performance indicators (such as time taken to address complaints) should also be set so that regular review could be conducted against such benchmarks. These are useful suggestions, although it is not clear they could be applied on a global scale since not all countries will have a developed or effective IRA for digital media industries.

H. Copyright liability and P2P intermediaries

The above discussion on NTD is predicated upon the online intermediaries having knowledge, whether actual or constructive, of the unlawful material, and therefore the ability to remove or block access to that material. But with P2P intermediaries, that is often not the case. A brief description of the types of P2P service providers or "P2P intermediaries" has been given above (see above p 7 et seq.). The purpose of this part is to look in detail at the attempts which have been made to hold P2P intermediaries liable for copyright infringement, and consider how courts have responded to these moves.

Liability for P2P software

The challenge for the entertainment companies has been to find a legal standard by which the authors and/or distributors of P2P software could be found liable for the transmission of works protected by copyright between P2P service users. In some jurisdictions it has not been possible to charge the authors or distributors of programs with primary copyright infringement as they do not make copies of the works: users make those 'copies'. Thus rather than primary infringement of copyright, secondary liability has been the focus of attention, most notably in the US, where it is framed as vicarious and contributory liability. In other jurisdictions, primary infringement has been the target through the test of 'authorisation of infringement' (Canada and Australia). In others still, related areas of the general law have been called upon (Netherlands).

Contributory and vicarious liability: the US.

While not appearing in the US Copyright Statute, two varieties of secondary liability have been recognised by US Courts: contributory and vicarious. Common to both is the requirement that there be a direct infringement by a primary infringer. Beyond that, contributory liability requires that the

infringer have knowledge of the infringement and that he/she make a material contribution to it.[94] This, it was said in *Aimster*, stemmed from a recognition that it would be impracticable and futile for a copyright owner to sue a multitude of infringers; the contributor or 'aider and abettor' could be sued instead. Vicarious liability requires that the infringer receive some financial benefit having some direct or indirect relation to the infringing conduct and that he/she has the right and ability to supervise the infringers.[95] This liability is said to have developed from an underlying notion of 'fairness'; when an individual seeks to profit from an enterprise in which identifiable losses are expected to occur, it is ordinarily fair and reasonable to place responsibility for those losses on the person who profits, even if that person makes arrangements for others to perform the acts that cause the losses.[96]

But vicarious and contributory liability will not attach where there are substantial non-infringing uses for a product. Thus in *Sony Corp. v. Universal City Studios v Sony Corporation of America*[97] the US Supreme Court had to consider whether Sony was vicariously or contributorily liable for the infringements carried out by users of the Betamax machine. The Court found that if vicarious liability was to be imposed on Sony, it must rest on the basis that it had sold equipment with constructive knowledge that its customers might use that equipment to make unauthorised copies of works protected by copyright. The Court found that: *'There is no precedent in the law of copyright for the imposition of vicarious liability on such a theory'*[98]. Thus, constructive knowledge that customers may infringe was not sufficient. The Court also drew on the '*staple article of commerce doctrine*' saying that '*The sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial non infringing uses.*' It was not necessary to say how much was commercially significant because the standard would be satisfied by one potential non infringing use, in this case the use of the Betamax machine for private non-commercial time shifting in the home. '*The Betamax is, therefore, capable of substantial noninfringing uses. Sony's sale of such equipment to the general public does not constitute contributory infringement of respondents' copyrights'*.[99]

Napster

So how, then, has secondary liability and the *Sony* test for 'substantial non-infringing uses' been

[94] *MGM v Grokster* 380F 3d 1154 (9th Cir 2004).
[95] It has been questioned as to the extent that the ability to control is a significant factor: Feder, "Is Betamax Obsolete? Sony Corp of America v Universal City Studios Inc in the Age of Napster" 37 Creighton L Rev 859.
[96] *Polygram Int'l Pub Inc. v. Nevada/TIG Inc* 855 F Supp 1314 (D Mass 1994). *Dreamland Ballroom Inc v Shapiro Bernstein &Co*. 36 F 2d 354 (2nd Cir 1929).
[97] 480 F supp 429 (C.D Cal 1979); rev'd 659 F 2d 963 (9th Cir 198d1); rev'd 464 US 417 (1984).
[98] Ibid p 439.
[99] Ibid p 456.

applied in the US courts to P2P intermediaries? *Napster*[100] was the first system to come under scrutiny in a case which was eventually heard by the US 9th Circuit Court of Appeals in 2001. The cataloguing process in Napster was carried out through an index maintained on the Napster service; any user request for a particular song or other work was routed via this centralised index. Napster sought to avoid the imposition of contributory liability by arguing that its software was capable of substantial non infringing uses (swapping of files which were not protected by copyright and/or to which the copyright owners had consented). The Ninth Circuit rejected that argument based largely on the grounds that Napster had a greater degree of knowledge of the underlying infringements than had Sony. Because Napster provided the centralised index, Napster, unlike Sony, had actual, not just constructive, knowledge of specific infringing materials. Where there was actual knowledge, it was irrelevant that the product was capable of substantial non infringing uses[101]. The Court considered that the provision of support services (the index system) constituted contributory infringement[102] and largely ignored the role that the distribution of Napster software played in the enterprise. On vicarious liability, the Court opined that Napster not only enjoyed a financial benefit - *'financial benefit exists where the availability of infringing material 'acts as a draw' for customers…Napster's future revenue is directly dependent upon increases in user base'* - but also that Napster had the right and ability to supervise the infringing conduct by blocking users' access to its service. The rest, as they say, is history.

Aimster

So Napster was found both contributorily and vicariously liable for the infringements by its users. The next case to come before the courts, which went to the US Court of Appeals for the 7th Circuit in 2003, was *In Re Aimster*.[103] As with Napster, Aimster made no copies of files on its servers. Information as to the location of files was kept on the computers of users, but it was part of Aimster's service that its software searched the computers of users on which files were located when a specific request was made. In addition all communications between the Aimster service and the users were encrypted by the sender by means of encryption software made available by Aimster. The Court took a different approach to that taken in Napster, saying that even if Aimster *could* show non infringing uses of the software, where it was *also* used for substantial *infringing* purposes, to avoid liability they would have to '*show that it would have been disproportionately costly for [it] to eliminate or at least reduce substantially the infringing uses.*' The approach was thus to balance the respective magnitudes or proportions of infringing uses against non infringing uses, and in so doing to look at the actual, and not just hypothetical, uses being made of the products or services: '*It is not enough…*

[100] *A&M Records v Napster* 9th Cir 2001.
[101] *Napster 2*, 239 F 3d at 1021.
[102] *Napster* 114 F. Supp. 2d at 919-20.
[103] 334 F.3d 643, 67 USPQ2d 1233.

that a product or service be physically capable … of a non-infringing use'.[104] Further it was necessary to determine not only what Aimster knew about the ways in which its software was being used,[105] but also what it had chosen not to know. In other words, the notion of willful blindness was rejected. *'Willful blindness is knowledge, in copyright law (where indeed it may be enough that the defendant should have known of the direct infringement)'*.[106] Aimster had argued that because it used encryption software, they did not know whether the system was used to swap infringing files by the users: *'Our point is only that a service provider that would otherwise be a contributory infringer does not obtain immunity by using encryption to shield itself from actual knowledge of the unlawful purposes for which the service is being used'*.[107] The Court also considered whether Aimster was vicariously liable by failing to eliminate the encryption feature of its system and monitor the use being made of the software. However, the Court felt it was not necessary to deal with this in detail because: '*its ostrich-like refusal to discover the extent to which its system was being used to infringe copyright is merely another piece of evidence that it was a contributory infringer'*.

Grokster

Aimster was thus held contributorily liable for infringement of copyright. But in the next case, *MGM v Grokster*,[108] heard by the 9th Circuit Court of Appeals in 2004, the technology had changed again. In Grokster, the system is decentralised, with each user maintaining an index only of those files which he or she wishes to make available to other users. When a user looks for a file, the software broadcasts a search request to all the other computers on the network. The collective results are passed back to the requesting computer. As with the other cases, direct infringement of copyright by the users was accepted. On the knowledge requirement for contributory infringement, the court said that where the product was not capable of substantial or commercially significant non-infringing uses, the copyright owner need only show that the defendant had constructive knowledge of the infringement. However, where the product *was* capable of substantial or commercially significant non-infringing uses, then the copyright owner must show that the defendant had *reasonable knowledge of specific infringing files and failed to act on that knowledge to prevent infringement*. Citing the example of the band Wilco, who had voluntarily made their music freely available for distribution using the software, the Appeals Court agreed with the District Court that the software was capable of substantial non infringing uses. This differs significantly from the test employed in *Aimster*, where, as discussed above, the court said that an important additional factor was how '*probable*' the non-

[104] Ibid p.653.
[105] The Aimster court stated: 'We therefore agree with Professor Goldstein that the Ninth Circuit erred in *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1020 [57 USPQ2d 1729] (9th Cir. 2001)'.
[106] *Casella v. Morris*, 820 F.2d 362, 365 [3 USPQ2d 1340] (11th Cir. 1987).
[107] 334 F.3d 651.
[108] Supra n 94. For a compilation of all the documents in this case see http://www.eff.org/IP/P2P/MGM_v_Grokster.

infringing uses of a product are.[109] According to the Court in *Grokster*, liability *also* required specific knowledge of infringement at the time at which a contribution was made to that infringement. In the absence of any centralised index under their control, Grokster had no such knowledge. Further Grokster did not materially contribute to the infringement*: 'they did not provide the 'site and facilities' for infringement and do not otherwise materially contribute to the infringement'*.

On vicarious liability, the Court noted that there was both primary infringement and a direct financial benefit (via advertising revenue). On the 'right and ability to supervise' the Court noted that in Napster it had been said that the *'ability to block infringers' access to a particular environment for any reason whatsoever is evidence of the right and ability to supervise*"[110]. However in *Grokster*, the court said that it did not appear from the evidence that there was the ability to block access to individual users: *'there is no registration and no log-in process so there is no ability to terminate access absent a mandatory software upgrade to all users'*. Thus, *'the sort of monitoring and supervisory relationship that has supported vicarious liability in the past is completely absent in this case'*[111]. In addition, the Court rejected the willful blindness theory put forwards in *Aimster*. The Defendants were thus found not liable.

The case has, of course, been referred to the Supreme Court. The question to be addressed is the issue of whether a defendant invoking the *Sony* defence has to show that the technology is capable of, or actually does, support substantially non-infringing uses. Oral arguments were heard on March 29, 2005, with the judgment expected to be handed down in early summer. One glance at the numbers of amicus briefs filed in the case indicates the strength of passion on all sides.[112]

BitTorrent

The difficulty in applying a proportionality test as suggested in *Aimster* (ie, what proportion of uses of a service are infringing as opposed to non infringing) can be well illustrated by looking at the development and subsequent use of BitTorrent. The technology underpinning BitTorrent has been explained above (p. 8). Of particular note are the reasons that Cohen (the developer), has given for the structure of the technology. Far from being designed as a program to enable the unlawful sharing of files, it is intended to lessen the bottlenecks that can occur when a large file is copied from a single computer – in other words, as a mechanism to improve the functionality of the Internet. Indeed, it is used by many for lawful purposes. For instance, Peter Jackson, the producer of the *Lord of the Rings* film trilogy is currently producing a remake of *King Kong.* During this process he

[109] *In re Aimster Copyright Litigation* 334 F 3d 643 (7th Cir. 2003) at 653.
[110] 239 F 3d at 1023
[111] *Grokster*, at 11744.
[112] See http://www.eff.org/IP/P2P/MGM_v_Grokster.

is keeping an online production diary which includes both text and video. As the video files are large, he is using BitTorrent to share the work of distributing the files.[113] BitTorrent is the major conduit for the legal and encouraged copying of open source Linux operating system files, and is also used to disseminate public domain works via Project Gutenberg. That, of course, does not mean that it is not used by others for unlawful purposes.[114]

Although the current focus of the content companies is on seeking to contain and close down BT torrent sites and hubs,[115] an MPAA spokesman has apparently said that Cohen (BitTorrent's developer) is under scrutiny for continuing to develop the software *'and making it easy to steal copyright material*.'[116]

Safe Harbor

In addition to the arguments concerning contributory and vicarious liability, the US courts have opined on the 'safe harbor' provisions to be found in the DMCA which can exempt qualifying service providers from monetary liability for direct vicarious and contributory copyright infringement and limit injunctive relief[117] so long as stated conditions are met.[118]

Napster

In May 2000 Patel J[119] considered the position of Napster in relation to Section 512 of the DMCA which addresses the liability of online service and Internet access providers for copyright infringements occurring online. Napster argued that it was a service provider within the meaning of s. 512(k)(1)(A) of the DMCA. This provides that the term 'service provider' means *'an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received*.' Napster claimed that it offered the *'transmission, routing, or providing of connections for digital online communications*' by enabling the connection of users' hard-drives and the transmission of MP3 files 'directly from the host hard drive and Napster browser through the Internet to the user's Napster browser and hard drive.' The Court was not wholly convinced saying that *'the court assumes, but does*

---

113 Kong is King.net|King Kong|Peter Jackson's Production Diary, at http://www.kongisking.net/kong2005/proddiary.
114 It has just been reported that an Australian ISP has had its offices raided in what appears to be the first action brought concerning the use of BitTorrent technology for copyright infringement in Australia.
http://www.zdnet.com.au/news/0,39023165,39184042,00.htm.
115 See n 10 supra.
116 Fonda, "Downloading Hollywood", TIME, Feb. 14, 2005.
117 To the degree specified in DMCA subsection 512(j)(1)(B).
118 These are to be found in DMCA s. 512(a).
119 Not Reported in F.Supp.2d Page 12000 Copr.L.Dec. P 28,072, 54 USP.Q.2d 1746, 2000 WL 573136 (N.D.Cal.)

not hold, that Napster is a 'service provider' under subparagraph 512(k)(1)(A)'[120].

Napster claimed that its business activities fell within the safe harbor provided by subsection 512(a). Liability of the service provider is limited where *'the material is transmitted through the system or network without modification of its content*'. The Court found this provision inapplicable as the files were not transmitted 'through the system' within the meaning of the statute, but through the Internet. Thus Napster did not qualify for the safe harbor provisions.

In August 2000, Patel J,[121] faced once again with an argument by Napster for eligibility under the safe harbor provisions, found that as Napster satisfied the objective test for constructive knowledge (Napster had reason to know about infringement by third parties), a finding which put to an end to the *'defendant's persistent attempts to invoke the protection of the Digital Millennium Copyright Act, 17 USC. ß 512 as this subsection expressly excludes from protection any defendant who has [a]ctual knowledge that the material or activity is infringing'* [122]or *'is aware of facts or circumstances from which infringing activity is apparent.'*[123] The court went on to say that Napster had *'failed to persuade this court that subsection 512(d) shelters contributory infringers.'* This finding was a step too far for the 9th Circuit which, said in February 2001 that: '*We need not accept a blanket conclusion that § 512 of the Digital Millennium Copyright Act will never protect secondary infringers*'.[124] *' We do not agree that Napster's potential liability for contributory and vicarious infringement renders the Digital Millennium Copyright Act inapplicable per se. We instead recognize that this issue will be more fully developed at trial*'.[125]

Aimster

We turn now to Aimster's claim to be eligible for the safe harbor provisions. The District Court Judge ruled that Aimster met the definition of an Internet service provider as found in

[120] DMCA s. 512(k)(1)(A) provides: As used in subsection (a), the term 'service provider' means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material sent or received. The Napster Court noted that in *Universal City Studios, Inc. v. Reimerdes*, 82 F.Supp.2d 211, 217 & n.17 (S.D.N.Y 2000), one Defendant had sought protection under subsection 512(c). Although the Court noted in passing that the Defendant offered no evidence that he was a service provider under subsection 512(c), it held that he could not invoke the safe harbor because plaintiffs claimed violations of 17 USC section 1201(a), which applies to circumvention products and technologies, rather than copyright infringement.
[121] 114 F.Supp.2d 896.
[122] DMCA s. 512(d)(1)(A).
[123] DMCA s. 512(d)(1)(B).
[124] The Court quoted inter alia Wright, "Actual Versus Legal Control: Reading Vicarious Liability for Copyright Infringement Into the Digital Millennium Copyright Act of 1998", 75 Wash. L. Rev. 1005, 1028-31 (July 2000) with approval where the author said '[T]he committee reports leave no doubt that Congress intended to provide some relief from vicarious liability'.
[125] The Court noted that the Plaintiffs had raised and continued to raise significant questions under the DMCA, including: (1) whether Napster is an Internet service provider as defined by 17 USC. s. 512(d); (2) whether copyright owners must give a service provider "official" notice of infringing activity in order for it to have knowledge or awareness of infringing activity on its system; and (3) whether Napster complies with s. 512(i), which requires a service provider to timely establish a detailed copyright compliance policy.

s. 512(k)(1)(B). This section provides that the term 'service provider' means *'a provider of online services or network access, or the operator of facilities, and includes an entity described in subparagraph (A)*' (see above). The District Court considered the various safe harbors potentially available to Aimster[126]:

- *The transitory communications safe harbor*:[127] The Court noted Aimster would not qualify for this as their system worked by allowing users to communicate and transfer files via privately created networks. Thus information transferred between individual users, but did not pass through Aimster's system.[128]
- *The system caching safe harbor*:[129] The court found that this section exempted a service provider from liability when liability results from the act of caching itself. This was '*simply not applicable in this case'*.
- *The information location tools safe harbor*:[130] The Court considered that Aimster did not meet the conditions under this safe harbor because, in order to apply, a service provider cannot have actual knowledge of the infringing material or activity, or, in the absence of actual knowledge, the service provider cannot be aware of facts or circumstances from which the infringing activity is apparent. If they did have such knowledge they must take steps to remove or disable access to the material.[131] Aimster had taken no such steps.

All of the safe harbors are subject to the proviso that the service provider must do what it can reasonably be asked to do to prevent the use of its service by 'repeat infringers'.[132] The District Court found that Aimster did nothing to comply with this requirement. The Court of Appeals agreed saying that, far from preventing infringement of copyright belonging to others, '*Aimster invited them to do so, showed them how they could do so with ease using its system, and by teaching its users how to encrypt their unlawful distribution of copyrighted materials disabled itself from doing anything to prevent infringement*.'

Aimster leaves us with the conclusion that the only relevant DMCA safe harbor provision – locational tool - thus crucially depends on a service provider which obtains knowledge (whether actual or constructive) of infringing activities then having the ability to removing the offending

---

[126] The hosting DMCA safe harbor is clearly inapplicable to all P2P intermediary cases as the intermediaries do not store copies of actual offending files: it is the P2P users who do so on their own computers.
[127] The *Transitory Communications Safe Harbor* provides that a service provider shall not be liable for copyright infringement by *"reason of the provider's transmitting, routing, or providing connections for, materials through a system or network controlled or operated by or for the service provider . . ."* provided a number of conditions are satisfied. 17 USC s. 512(a).
[128] The Court cited *A&M Records v. Napster,* No. C 99-05183, 2000 WL 573136 (N.D. Cal. 2000) *"even if each users' Napster browser is part of the system, the transmission goes from one part of the system to another, or between parts of the system, but not 'through' the system."*
[129] The *System Caching Safe Harbor* provides that a service provider shall not be liable for copyright infringement *"by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider."* 17 USC s. 512(b)(1).
[130] The *Information Location Tools Safe Harbor* provides that a service provider shall not be liable *"by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link,"* if the service provider meets three other specified conditions. 17 USC. s 512(d).
[131] 17 USC. s 512(d)(1)(C).
[132] 17 USC. s 512(i)(1)(A).

material. As we have seen, the ECD applies a similar notice and takedown regime, albeit in relation to hosts only, as it lacks a linking immunity provision. But a brief consideration of the technology shows that NTD is not satisfactorily applicable as a regime of protection to P2P intermediaries of the post Napster variety. Napster's centralized index meant that in theory it *did* maintain control over what files could be downloaded by users and so NTD was in principle applicable, even though, in practice, its attempts to implement takedown overwhelmed its resources, destroyed its business model and eventually resulted in its closure. Aimster said that it could not comply with any NTD provisions as it simply did not know what the users were doing, due to the encryption technology it supplied, but was nonetheless rebuked and held liable for its self-imposed "willful blindness". But Grokster represents a fundamentally different architecture to Napster and Aimster. Takedown notices could only be served on Grokster after all effective control they had over the making or storing of copies had already been ceded to users. In the *Grokster* case, the safe harbor provisions were not considered in detail; the Court seems to have accepted that as Grokster could not know of the infringing uses at the time at which the infringement took place, the issue of takedown could not arise. It would thus seem that attempts to invoke an NTD procedure to shield a P2P intermediary from liability where the service operated is of the decentralized post-Napster type are simply inappropriate.

O*ther jurisdictions*

There has been a surprising lack of legal actions involving P2P intermediaries in jurisdictions other than the US and the UK to date. It may be that the entertainment companies are waiting for the decision by the Supreme Court in *Grokster,* although the weight accorded to this decision in other jurisdictions remains to be seen.

Netherlands

The Supreme Court of the Netherlands in The Hague has considered the liability of the makers of the KaZaA software for infringement of copyright in works swapped between its users in *Buma/Stemra v Kazaa.*[133] The court did not deal with the broad issue of legality of file sharing programs but did find that KaZaA was not liable for copyright infringement in music or films swapped on its software.

It was argued that KaZaA had infringed copyright by enabling their users to download music files

[133] Nr. AN 7253 Case No.: CO2/186HR

using their software.[134] A number of avenues were explored in exonerating KaZaA:

- First, and to the extent that acts infringing copyright had been performed, these were by the users of the system, and not by KaZaA;
- Second, the provision of facilities for the publication or reproduction of protected works was found not in itself to be an act that falls under the (primary) publication or reproduction rights in the Netherlands;
- Third, and referring to the evidence had been provided that there were non-infringing uses of the program, it was said that the provision of the computer program by KaZaA *'could not be assessed as being illegal'*;[135]
- Fourth, KaZaA could not be found liable as a 'co-disclosing' party for the publications by users; and
- Fifth, and on whether KaZaA was individually infringing copyright, it was said *that 'the situation where…the software provider does not make individual publications in the localised peer to peer file sharing networks '* will not be liable for infringement. Even although KaZaA provided 'assisting software' for passing on music which made use of the supernodes in the system, it is the users who *'pass on the music mutually' using the software they have obtained*'.[136]

The Court concluded that *'the provider of peer to peer software is …not liable as such to the extent that such provider does not make any works public or provide them publicly himself*'.[137]

On indirect liability for copyright infringement (and referring to the *Buma/De Vries* decree of 1957)[138] the Court said that there was no liability purely based on 'owning the location' or providing the facilities.

Finally, and in opining as to when a service provider might be liable, the court referred to *Scientology v XS4ALL*,[139] a case in which the court had found that the service providers did not name any publications themselves and went on to say: *'this does not alter the fact that the service provider who does not make any publications and reproductions itself may, pursuant to due care appropriate in social and economic life, nevertheless be committed to cooperate and take adequate measures when the service provider is notified of the fact that one of the users of its computer system is committing copyright infringements or otherwise acting unlawfully through the service provider's home page*'.

---

[134] Ibid para 4.9.
[135] Ibid para 4.0.
[136] Ibid para 5.11.
[137] Ibid para 5.15.
[138] Supreme Court 8 March 1957, NJ 1957, 271 (Buma/De Vries).
[139] *Scientology v XS4ALL* Court of The Hague 9 June 1999 NJ Kort 1999, Information Law/AMI 1999, at p.110.

The Court concluded saying: *'the provider of peer to peer file sharing software as the one at issue cannot be itself held liable for infringement of copyright. The provider may in certain circumstances be responsible for a wrongful act'*.[140]

So here it seems the general law of delict/tort may be applicable to fix liability on a P2P intermediary or at least to require it to take action where it knows of infringing uses. The Court clearly thought that where a P2P intermediary was informed that its program was being used for unlawful acts, then appropriate measures may have to be taken. However, this would appear to fall far short of an NTD regime, the focus seemingly rather being on the individual who was committing the copyright infringement. Under these circumstances, there may, for instance be a requirement to terminate the user's account, though it is hard to see how useful this can be in relation to services like KaZaA or BitTorrent where the subsequent use the P2P user makes of the P2P software once downloaded is completely outside the control of the P2P intermediary. The most KaZaA could do, for example, is prevent a user downloading an upgraded version of the P2P software. With BitTorrent, where many BT clients are available from different sources, even this could not be guaranteed. Again, the language of the court and the fallback on some kind of NTD-like regime as limitation on P2P immunity, seem more appropriate to Napster type P2P services than the decentralised services now universally deployed.

Canada

Society of Composers, Authors and Music Publishers of Canada v Canadian Assn. of Internet Providers[141], although not directed at P2P intermediaries as such, is interesting for the position taken with respect to authorisation of infringement (a primary rather than secondary infringement of copyright). This is a standard of liability which has been equated with the US contributory and vicarious liability in that it seeks to place liability not on the actual infringer, but on a third party who may in some way be responsible for the underlying infringement. It is a standard to be found not only in Canada, but other jurisdictions as well, including the UK and Australia. The Canadian case concerned the question as to who should compensate copyright owners for music and other works originating from a foreign country but downloaded in Canada. The collecting society wanted to collect royalties from ISPs located in Canada, arguing that it was the ISPs that infringed the copyright owners' right to communicate the work to the public, and to authorise such communication. In response to this charge, the Canadian ISP association argued that they neither communicated nor authorised anyone else to communicate these works, being simply conduits. The Court, having decided that *'each*

[140] Buma/Stemra v KaZaA para 5.40.
[141] [2004] 2 SCR 427.

transmission must be looked at individually to determine whether in that case an intermediary merely acts as a conduit for communications by other persons, or whether it is acting as something more' concluded by saying that, generally speaking, *'with respect to most transmissions, only the person who posts a musical work communicates it.'*[142]

So it is the person who posts the music file or other work who is liable for communicating that work. But could the ISP be said to be "authorising" infringement where, under Canadian legislation, authorising a communication by telecommunication is an infringement of s. 3(1) of the Copyright Act?

In discussing this point, the Court referred to *CCH v Law Society of Upper Canada*,[143] a case concerning the provision of a photocopier in the library of the Law Society of Upper Canada. On authorisation of infringement, the Court in the instant case quoted *CCH* with approval '*… a person does not authorise infringement by authorising the mere use of equipment that could be used to infringe copyright. Courts should presume that a person who authorises an activity does so only so far as it is in accordance with the law…this presumption may be rebutted if it is shown that a certain relationship or degree of control existed between the alleged authorise and the persons who committed the copyright infringement*'.[144]

Thus even where an ISP has knowledge that its facilities may be used for infringing purposes, that does not make the ISP liable for authorising the infringement unless it purports to grant to the person committing the infringement a licence or permission to infringe. An intermediary would have to *'sanction, approve or countenance more than the mere use of equipment that may be used for infringement. Moreover an ISP is entitled to presume that its facilities will be used in accordance with the law'*.[145] The Court did go on to say that liability for infringement of copyright *'may well attach if the activities of the ISP cease to be content neutral e.g. if it has notice that a content provider has posted infringing materials on its system and fails to take remedial action*'.[146]

If these same standards were applied to P2P intermediaries, then it would be unlikely that they would be found to be liable for authorisation of infringement. A P2P intermediary may make the software available that is subsequently used for infringing purposes. But under the test articulated above, it would be very hard to argue that the authorisation extended to acts by users beyond what

[142] Ibid para 111.
[143] [2004] 1 S.C.R. 339, 2004 SCC 13.
[144] Supra n 141 para 122
[145] Ibid para 124.
[146] 'The knowledge that someone might be using neutral technology to violate copyright… is not necessarily sufficient to constitute authorisation, which requires demonstration that the defendant did 'give approval to; sanction, permit; favour encourage (CCH para 38) the infringing conduct. ..'. 'notice of infringing conduct and a failure to respond by 'taking it down' may in some circumstances lead to a finding of 'authorisation''. Ibid para 127.

was permitted by law (except perhaps in situations such as was the case in *Aimster*, where clear instructions were given on how to use the software and those instructions related specifically to infringing uses). Further, as has been discussed above, P2P intermediaries of the post-Napster type tend to have neither knowledge of, nor control over, the activities of their users subsequent to download of the P2P software.

In both *Bumra Stemra v KaZaA* and *Society of Composers, Authors and Music Publishers of Canada v Canadian Assn. of Internet Providers*, it was said that where there was knowledge of the infringing activity, then steps may have to be taken to remove the infringing material. This of course brings us back to the crucial architectural differences between Napster and Grokster. Napster was required to remove references to infringing files from the index held on its servers on the grounds that it had knowledge of the infringing files, and was thus technically capable of removing them from the index. In practice, it collapsed under the burden of so trying. But with KaZaA/Grokster, and similar decentralized services, stopping of infringing uses appears not to be possible. Such services do not know of infringements at the time at which they are carried out, and there appears to be currently no mechanism for them so finding out. In oral argument in the ongoing Australian suit against KaZaA (see below), the record industries have suggested that the KaZaA software should be modified such that before files are uploaded by KaZaA users, they must first be notified to KaZaA, who can then check, for example, to see if they are non infringing, and authorize them for distribution.[147] Such a suggestion however seems so impractical as to be tantamount to closing KaZaA down.

Australia

Australia, another jurisdiction where there is ongoing litigation against KaZaA, also uses the test of 'authorisation of infringement'. However, application of the test might yield a different result to that obtained in Canada. In Australia, recent amendments to copyright law in the Copyright Amendment (Digital Agenda) Act have changed the provisions relating to authorisation of infringement of copyright. To an extent the new provisions codify the law as it evolved in *University of New South Wales v Moorhouse.*[148] This case concerned the provision of a photocopier in a University Library. The Australian Court found that by providing this facility in the library, the University had thereby authorised the infringement of copyright by its users. The Court considered that the term 'authorise' meant *'sanction, approve, countenance or permit'*.[149] Express permission to infringe copyright was not necessary: *'inactivity or indifference, exhibited by acts of commission or omission'* might be enough to

[147] See "Music industry attacks pirates", 23 March 2005, *Australian Financial Review*.
[148] (1975) 133 CLI 1.
[149] ibid

infer authorisation. It was however necessary that the person authorising the infringement knew, or had reason to suspect that the infringing activity would take place.

'It seems ... to follow from these statements of principle that a person who has under his control the means by which an infringement of copyright 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 authorise any infringement that resulted from its use.' [150]

The Court noted that the photocopiers were used extensively for activities that did not infringe copyright. However, unlawful copying was likely to occur unless mechanisms were put into place to stop it. The University had grounds to suspect that infringement would occur and could control the purposes for which the machines were used. The result was that where people used the machines to infringe copyright it could be said that the University authorised them to do so. The recent amendments to the Australian Act, drawing on the principles enunciated in this case, now list some of the factors that must be taken into account when deciding on authorisation. These include:

- the extent of a person's power to prevent the infringement;
- the relationship between the actual infringer and the person purportedly authorising that infringement; and
- whether any reasonable steps were taken by the person purportedly authorising the infringement to prevent that act.[151]

From this it has been argued that: *'in the case of P2P sharing, if the distributor of the P2P software has reasonable grounds to suspect that infringing activities were likely to take place, and they have the power to prevent or control those activities and do not take reasonable steps to do so, then they have authorised these infringements. This situation would therefore amount to copyright infringement under s 101 of the Copyright Act'*.[152]

But this conclusion does beg a number of questions. It assumes that the P2P intermediary has the "*power to prevent or control*" those infringing activities. Does this require the P2P intermediary to have that power at the time of the infringing act? As has been discussed above, whereas Napster did have such power, at least in theory, it would appear to be acknowledged (at least so far) that Grokster does not. When is the knowledge, whether actual or constructive, relevant? At the time of the infringing act? In which case P2P intermediaries will generally lack any power to prevent or control

---

[150] Supra n 148 at p.21.
[151] Copyright Amendment (Digital Agenda) Act s 101(1A).
[152] Douglas, "Copyright and PtoP music file sharing. The Napster case and the argument against legislative reform" Murdoch University Electronic Journal of Law Volume 11, Number 1 (March 2004) available at http://www.murdoch.edu.au/elaw/issues/v11n1/douglas111.html

infringements in particular where their architecture resembles that in issue in Grokster. Or can it be extended to mean knowledge at the time that P2P software is made available to potential infringers, or downloaded by a particular infringer? If so, should P2P download sites be required to try to prevent download by named repeat infringers notified to them by rightsholder industries? What liability would they incur if (as would be inevitable) downloaders disguised their name and other identifying features such as IP address?

In addition, what is meant by taking reasonable steps to limit the use of the means of infringement to legitimate purposes? In *Moorhouse*, this line of argument led to lengthy copyright warnings being posted on public photocopiers in Australia (and in other jurisdictions including the UK). Would warnings concerning the use of the software by users (eg,. that it should not be used for infringing purposes) be sufficient? (Such warnings in fact already exist in the end-user license agreements (EULAs) of most services such as KaZaA, but are of course, universally flouted by users – as indeed, arguably, so are notices on public photocopiers.) Or might there be a higher test imposed, such as an obligation to develop the software in such a way to ensure that it could not be used for infringing purposes? As noted above, this is one of the directions the recording industry would like to see actively promoted. It has however been argued to the contrary during the hearings that rather than applying the *Moorhouse* test, the standard laid down in the British case of *CBS Songs v Amstrad*[153] would be more appropriate. Here, the English Court found that the makers of a twin tape deck did not 'sanction, countenance or approve' the making of unauthorised copies of songs using the technology. Warnings were included with the product indicating that unauthorised copying of protected songs was unlawful. This might suggest again that, in order to avoid liability, rather than including demonstrations on how to use the technology specifically mentioning sharing of music files (as was the case with Aimster) P2P intermediaries should include disclaimers stating the technology should not be used for such infringing purposes. Yet in practical terms, neither disclaimers nor active imposition of contractual conditions by EULA is likely to make any difference to the actual level of infringing use of P2P services, and such obligations are highly unlikely to satisfy the rightsholder industries.

Much has been said during the course of the hearing in *Buma/Stemra v KaZaA* with assertions and counter assertions being made by both sides. For instance, it has been claimed that KaZaA contains a central indexing function which could mean that control could be exerted over the use of the system. This has been vehemently denied by the defendants. It has also been suggested, as noted above, that KaZaA should be subject to some sort of licensing system; only licensed content could be placed on the system. Understandably the free speech advocates have hotly contested this

[153] [1988] AC 1013.

suggestion. Arguments in the case have now closed with the judgement expected to be handed down during the coming weeks. Whatever the result, it will give much food for thought: a comparison between the instant case and whatever the US Supreme Court has to say in *Grokste*r may even give an indication as to the extent to which jurisdictions are converging or diverging on this most vexed issue.

I. Suing downloaders and uploaders rather than P2P intermediaries

In tandem with their efforts to hold P2P intermediaries accountable for copyright infringement, the entertainment companies have also threatened or initiated law suits against individuals in an expanding range of jurisdictions, including the USA, Canada, the UK, Germany, France, Austria, the Netherlands and Japan.[154] Since most file-sharing is carried out by users pseudonymously or anonymously, this has lead to a corollary growth in litigation around whether, and under what circumstances, ISPs and hosts should reveal the true name and personal details of file-sharers. The implications of these cases for privacy rights are dealt with briefly below. It is worth noting that, once identified, almost all individuals sued have settled rather than face the risks and expense of going to court. The settlement culture can be seen as unfortunate for many of the reasons explored in the literature around SLAPP (Strategic Litigation against Public Participation) law suits[155]primarily that possible defenses for those sued are not being aired in court and therefore not available as practical guidance to other defendants; which itself may increase the likelihood of settlement out of fear of unquantified risk. As noted above, there is clear evidence that some cease and desist letters are being served which are faulty in both fact and law, yet these are almost never publicly challenged, the "Chilling Effects" clearing house site being the major exception[156].

Exemptions from liability for downloading : Canada

It has been the uploaders who have been the focus of attention by the big record companies. This is not only because it is the uploaders who make the works available for others to illegally copy, but also perhaps because downloading is not unlawful in all jurisdictions. In Canada, in 2003, the Copyright Board[157] found that s. 80 of the Canadian Copyright Act creates an exception to the exclusive reproduction right and makes lawful private copying onto audio recording media. The

[154] For further discussion see Waelde C and MacQueen H, "From Entertainment to Education: The Scope of Copyright" [2004] IPQ 259, 270.
[155] Information about SLAPP can be found at http://www.cyberslapp.org/intro.cfm
[156] See n 80 supra.
[157] Copyright Board Canada Private Copying 2003-2004 DOSSIER : *Copyright Act*, subsection 83(8) Tariff of levies to be collected in 2003 and 2004 on the sale of blank audio recording media, in Canada, in respect of the reproduction for private use of musical works embodied in sound recordings, of performer's performances of such works and of sound recordings in which such works and performances are embodied. Decision of the board. December 12, 2003.

exemption is only applicable for the private use of the person making it (it does not, for example, extend to making a copy of a CD to give to a friend). Downloading (or end copies) are thus not infringing copies where downloaded for personal use, even where the source copy is an infringing copy. The corollary is a levy system: '*All private copying is now exempt, subject to a corresponding right of remuneration*'.[158]

France

In France too, downloading and copying of downloaded music and films onto CDs has recently been found to be lawful, even where some of the resulting CDs may be lent to or played in the presence of one or two friends.[159] In a case decided on March 10, 2005, the Montpellier Court of Appeals so found when faced with a case where an individual was sued by music and record companies (including Buena Vista, Columbia and Disney) for downloading films and music from the internet and copying these onto CDs: the Court found that the use was not of a commercial nature.[160] This finding immediately raises the following question: with how many persons must downloaded copies of music and films be shared in order to exceed the scope of legitimate private use and become infringing under French law? Although the case concerned the sharing of music and films copied onto CDs, similar reasoning might be applied to the 'sharing' of files over the Internet.

BitTorrent, downloading and uploading

Jurisdictions where downloading is legal, but uploading is unlawful, present problems in the world of P2P, where most users take on both roles. In some systems, the software itself may automatically designate certain users as "supernodes", for example, which may conceivably involve extra vulnerability to legal liability. To make matters worse, with certain P2P services, it may be unclear as to whether users are uploaders, downloaders or both at the same time. Take the example of BitTorrent (BT). Here, users are by default both downloaders and uploaders. Does this make every BT user potentially liable for infringement for *uploading*, even in those jurisdictions where *downloading* is in certain circumstances legal? Might there be room for the argument that the amount that is copied in the process of uploading is an insubstantial part of the whole of the work as a whole (both qualitatively and quantitatively) and thus uploaders should not be liable for infringement? This would leave the question as to whether there is an infringement by the downloaders in those

[158] Ibid p.22.
[159] The Court applied article L. 122-5 of the French Intellectual Property Code: Once a work has been disclosed, the author may not prohibit: 1. private and gratuitous performances carried out exclusively within the family circle; 2. copies or reproductions reserved strictly for the private use of the copier and not intended for collective use.
[160] Decision at http://www.juriscom.net/documents/camontpellier20050315.pdf.

jurisdictions in which the 'bits' are reconstituted to make a whole.

Hiding the infringers

Suing individual uploaders and downloaders brings its own problems, not least of which is the matter of identifying the individuals. As discussed below, courts have taken different attitudes to requiring disclosure of the identity of individual users. But as P2P services have developed, so it has also become possible for users to be hidden successfully by the very technology that they are using to files with each other. The best current example is Freenet, a technology explained as follows by Ryan Roemer:[161]

> *'Freenet users insert files into the Freenet. Users create a 'key' for the Freenet file such as 'freenet:the_constitution.txt,' and insert the file into their node. The file is then stored on one or more local Freenet nodes. As Freenet users request the new file, neighboring nodes make additional copies of the file, distributing it across the Freenet. More popular files spread to more and more servers across the Internet… since Freenet servers have a limited storage capacity (determined by the node operator), less popular files get pushed out of servers and eventually drop off the Freenet altogether. Thus, Freenet does not rely on specific nodes to serve requested files, but instead acts as a large "cache," bringing more popular files closer to the users who want them.'*

Files in Freenet are inserted in encrypted form, and communications between nodes are encrypted. Retrieval of a file by Freenet is however slow and ponderous as files cannot be searched for by name such as "Britney.MP3". Instead, each file is assigned a unique ID number as it is inserted and it is this ID that must be searched for. As there is no central database linking filenames to IDs, it is thus impossible to locate a file by its filename, or know what the file with a particular ID is without first downloading it and opening it.

The users of Freenet remain anonymous through its architecture, whereby each node only knows the Internet Protocol address of its neighbours. *'When a file is retrieved or transmitted to a Freenet client, only the last node that contacts a monitoring node might be identified. However, there is no way of knowing whether that last node originated the file, or just passed on a "cached" copy from an earlier node. As files are requested and cached across the network, a node operator's server storage is used <u>without the node operator's knowledge or control</u>. A node operator cannot remove or determine what files are being served off of the node at any given point.'*[162]

[161] Roemer R. "The Digital Evolution: Freenet and the Future of Copyright on the Internet", 2002 UCLA J.L. & Tech. 5.
[162] Ibid section A.

Thus, although IP addresses can be connected to real world IDs by application to the ISP that issued them, Freenet makes the process of identification extraordinarily hard. If Bob downloads infringing files on Freenet by connecting to Bill in Toronto who's connected to Derek in Australia who's connected to Clive who's an RIAA snoop in California, then the RIAA will need to subpoena ISPs along the whole chain in order to find who Bob is. Furthermore any Freenet user sued for having infringing files (or parts thereof) on his hard drive can validly claim that he did not know what those files were (due to the encryption) and that they had been passed on by some other Freenet user and were essentially in transit without his knowledge, intent or control.

Identifying the infringers

Freenet brings us naturally to a discussion of how to identify the users of less impregnable P2P systems. The key question here is what standard should be applied to a request from a rightsholder to disclose the identity of an alleged or suspected file-sharer. Many jurisdictions explicitly or implicitly protect the privacy of citizens sending or receiving electronic communications. In the US and some other states, the right of anonymity for the purpose of political expression and interchange is constitutionally protected. Yet most jurisdictions also have fairly standard judicial, or administrative procedures to disclose evidence necessary to pursue litigation. The question is how these two values, privacy and anonymity vs. access to natural justice for parties whose rights have been infringed, should be resolved.

A crucial issue is whether disclosure should be mandated by courts even where no litigation has been commenced or is likely to be commenced. If this is allowed, there is a danger of suppression of the rights of defendants, since most file-sharers, faced with the superior resources of the recording and other entertainment industries will give in and settle once he or she is identified, rather than take any mistake in identity or of fact or law to court (see NTD discussion, above). It is widely reported that legal actions alleging unauthorised file-sharing have been commenced against elderly and deceased person, as well as a 12-year-old child. There seems to be a need for procedures to prevent initiation of disclosure actions against the wrong defendants, or becoming tantamount to routinised Cyber-SLAPPS[163]. Another crucial issue is how much evidence of infringement should be required to justify disclosure of personal identity. Should disclosure be a routine step before a full trial of the evidence, or should there be a fairly high standard of proof required before the shroud hiding identity can be unwrapped? Such states as have so far heard litigation on these points have varied considerably in the approach taken.

[163] See http://www.cyberslapp.org/intro.cfm.

In Europe, nothing in the ECD provides a mandatory framework for when disclosure of the identity of a user of an ISSP is legal, although other EC legislation such as the Data Protection Directive is of course relevant. There has been one rather unsatisfactory reported case in the UK thus far, *Totalise v Motley Fool*[164]. *Totalise* was in fact a libel rather than a copyright case, in which an unknown person, ZedDust, had made apparently libelous comments about Totalise, a US ISP, in online investment forum, whose content was provided by Interactive Investor (II) but was hosted by Motley Fool (MF) on their very popular investment advice website. The focus of the first *Totalise* case was mainly whether MF were entitled to disclose, given the compunctions of the EC Data Protection Directive which normally requires consent by the data subject to the sharing of personal data such as names and addresses. The Court had little trouble in saying that an exception in the UK Data Protection Act 1998 s. 35 allowed disclosure without consent "where disclosure is required … by any rule of law or by order of court." Since *Norwich Pharmacal*[165] broadly authorized courts to make such disclosure orders, this would trump any DP obligations. Two other important issues were raised. First, the High Court declared with very little argument that a disclosure order could be made even though no litigation had been commenced. Second, a statement that privacy of users would be respected in the MF privacy policy "*must take second place*" to the obligation of disclosure on MF since they had "*become involved in the tortious acts of others*". Only the most desultory effort was given to balancing the right of privacy against the needs of justice. "*To find otherwise would be to give the clearest indication to those who wish to defame that they can do so with impunity behind the screen of anonymity made possible by the use of websites on the internet.*" Given this judicial attitude, it is hardly surprising that when the BPI requested the High Court in March 2005 to order Internet Service Providers (ISP) to reveal the identity of 28 persistent file sharers, there seems to have been no attempt at argument in court either from the ISPs, the filesharers or any other group, and that the orders for disclosure were all granted without opinion being issued. (Subsequently, interestingly, all 28 settled out of court for reduced damages, a good example of "volume business".[166])

A later *Totalise* case concerning costs[167] also raised interesting issues. Basically, II complained that as it was MF, not they, who had insisted on defending the case in court rather than just handing over the ID details without any court order, II should not be asked to pay any of the costs of the action (which are usually awarded against the losing party). In response, the Court of Appeal held that the party asked to disclose should *not* have to meet the costs of the court order for disclosure if that party:

- had a genuine doubt that the applicant was entitled to disclosure;

---

[164] [2001] EMLR 29.
[165] [1974] AC 133 (HL).
[166] The activities of the RIAA in pursuing infringers have led one individual to opine that the RIAA runs its lawsuits in a manner akin to a volume business. At http://b2fxxx.blogspot.com/2005/03/meet-john-doe.html.
[167] Court of Appeal, 19 December 2001, unreported.

- had genuine doubt that they might be legally obliged not to disclose (eg by DP obligations);
- could be subject to legal proceedings if they disclosed voluntarily (as was possible here since disclosure breached the terms of the privacy policy); and
- would be infringing the legitimate interests of *others* by making disclosure.

In the end as a result, the costs order against II was overturned. This (under-reported) analysis is more helpful than the original case though it is still not exactly the balance between privacy and justice that a freedom of speech advocate would hope for.

In the USA, the terrain is different again. Although anonymity is normally treated as an important civil right, copyright disclosure cases are treated differently than cases involving ISPs and other types of anonymous defendants, such as alleged defamers[168]. In the US, a special fast-track subpoena procedure for disclosure of the identities of copyright infringers is available under the DMCA, s. 512(h). Basically, a properly formulated subpoena submitted by the rightsholder empowers the service provider (ISP or host) to disclose the ID of the anonymous or pseudonymous person in question, "notwithstanding any other rule of law". Thus, scrutiny by the court of the merits of the disclosure is usually wholly circumvented. Compare ordinary cases of disclosure by ISPs in the US, such as *Dendrite v John Doe No 3*[169]. This concerned whether Yahoo! should disclose the identity of an anonymous subscriber who was alleged to have libeled Dendrite, broken his contract and misappropriated trade secrets. John Doe was in fact a "whistleblower" alleging misbehaviour within Dendrite of public interest, which perhaps explains the court's sympathetic attitude. The Court stated *ab initio* that "*the court must balance the defendant's First Amendment right of free speech against the strength of the prima facie case presented*" and carefully applied a four part test to ensure that anonymity was not lightly prejudiced; the most important prong of this test being that the plaintiff had to show essentially a potentially winning case against the defendant before disclosure would be ordered. Compared to the DMCA procedure, the difference in standards is remarkable[170].

What *have* made it into the US courts, however, have been attempts to use the special subpoena provisions to bring Internet access providers into the same disclosure regime as "service providers". In the controversial case of *RIAA v Verizon*[171] the RIAA attempted to get Verizon, who were acting

---

[168] See *Dendrite v John Doe, No 3* 775 A.2d 756 (N.J. App 2001).
[169] Ibid.
[170] It was argued in *Verizon* (infra) that s. 512(h) was in fact an unconstitutional breach on freedom of speech; however the court did not address this argument.
[171] See for the initial decision upholding the subpoena against Verizon sought by the RIAA, *In re Verizon Internet Services*, 2003 US Dist. LEXIS 681 (D.D.C. 2003). That decision was successfully appealed by Verizon on February 2004: see http://www.eff.org/legal/cases/RIAA_v_Verizon/opinion-20031219.pdf. The RIAA are now seeking to appeal to the US Supreme Court. The EFF amicus brief explaining why Verizon should not be regarded as a "service provider" for the purpose of the DMCA can be found at http://www.eff.org/legal/cases/RIAA_v_Verizon/20030516_eff_amicus.pdf .

as a mere conduit, *not* a host or ISP, to disclose names of alleged infringers. This attempt was eventually rejected, after the US Court of Appeals reversed the lower court[172] on the grounds that Verizon did not fit the definition of "service provider" under s. 512(h). Although certainly an "ISP", the court found that Verizon had merely transmitted the infringing material not stored it on its servers. Similarly in the more recent case of *Charter Communications v RIAA*[173], the 8th Circuit ruled that the provision allowing copyright holders to subpoena ISPs did not apply to cases in which an ISP served only as a "conduit" for allegedly infringing materials, but rather only to cases in which an ISP actually hosted, cached, or linked to allegedly infringing materials.

Serious attempts have been made by courts in countries other than the US and the UK to balance the privacy rights of file-sharers with rights of access to justice by rightsholders. In Canada, the leading case is *BMG v John Doe*[174]. Various recording companies sought disclosure of the IDs of a large number of alleged filesharers. After a robust investigation, the court threw the applications out. Although their scrutiny was based on the same basic authority as the UK court's in *Totalise* – namely *Norwich Pharmacal*[175] – their approach was very different. The Canadian Court derived from *Norwich Pharmacal* five criteria to be met before an order of disclosure: (a) the Applicant had to establish a prima facie case against the alleged infringer, (b) the intermediary disclosing had to be more than just an innocent bystander, (c) this must be only practical way of obtaining the identity of the alleged infringer, (d) the disclosing intermediary must be reasonably compensated, and, most important, (e) "*the public interests in favour of disclosure must outweigh the legitimate privacy concerns*". In the event, an order of disclosure was denied mainly on the basis of the first criteria: evidence of alleged infringement was based on hearsay, unreliable and partial. A second problem was that there was no evidence of how a connection had been made between the pseudonyms of filesharers on KaZaA, and the IP addresses given to the ISPs for look-up and disclosure. Interestingly, the Court also opined that there was no clear evidence of copyright infringement, as the judgment of the Supreme Court of Canada in *CCH Canadian Ltd. v. Law Society of Upper Canada* had held that simply placing personal copies of copyright music files into shared directories accessible by other computer users was not *per se* infringement. In other words, the record companies needed to show not only that these *were* the people who had been downloading infringing copies, but also show that they had not *just* been copying or sharing them, legally, for their own private use, before an order for disclosure would be appropriate. Finally, the Court made the good point that looking up the identities behind dynamic IP addresses is by no means a trivial process, and that even if an account was identified, it might not

[172] See on the first instance case, Hilden J "Anonymity v Law Enforcement: the Fight Over Subpoenaing Alleged Downloader's Names from ISPs", a http://findlaw.com, October 1 2003.
[173] See http://www.ca8.uscourts.gov/opndir/05/01/033802P.pdf .
[174] 2004 FC 488.
[175] Supra n 157.

identify the actual user who downloaded illegally, for example, in a shared or wi-fi household. There was a serious possibility that an innocent account holder might be identified. In the end, therefore, the privacy interest outweighed the public interest favouring disclosure.

The Canadian case is perhaps the ideal model of how such cases should be approached and a balance struck. In Continental Europe, cases have also leaned against routine disclosure, with courts in Germany and Austria recently rejecting demands from record companies for disclosure[176]. A Munich appellate court recently declared that an earlier order allowing disclosure could not "*conceivably continue to stand*" on the grounds the ISP was not "an actual participant in the – alleged – infringement of copyright". The Viennese Court said that personal data could only be provided by the ISP in the case of a serious offence punishable with imprisonment of more than six months: in Austria, even uploading files for commercial purposes only earns a maximum six-month jail term. Given the emerging attitude of Continental legal systems (see above) that private downloading and even a small degree of private file-sharing is in principle legal, it is hard to imagine them being sympathetic (as in the Canadian *BMG* case) to requests for disclosure without good proof of commercial copying.

J. Alternate solutions

As has been commonly said lately, we now survey a playing field where, lined up on one side, the content industry assembles its team to assert its legitimate demands to control content in which it holds IP rights, to be remunerated for copies made, and to discourage the infringement of such rights. Facing them, we have a more diverse and perhaps less cohesive band of opposing interests. First, as asserted by organizations such as Creative Commons, there is the public interest in rights of access to material in the public domain, to comment on and use in limited legal ways non-public domain texts, to educational and scientific materials and to open source/"copyleft" materials. But secondly, there is also a more general public concern that law and regulation should not unreasonably hinder technological progress. Currently, the lawsuits which are intended to protect the legitimate interests of rightsholders are broadly viewed as having the less desirable consequence of restricting efficient development of P2P technologies. These technologies have tremendous potential to be socially useful, not only in the developed world where P2P litigation has so far taken place, but also in the developing world. Are there any means by which these competing interests can be reconciled?

It would seem, as discussed above, that existing standards for both primary and secondary liability

[176] EDRI-gram, No 2.25, 29 December 2004.

for copyright infringement are not well suited to meet the technological challenges raised by P2P services. Having surveyed developments in a range of key jurisdictions, these are but a summary of some of the reasons why:

- There seems no clear bright line globally as to whether P2P intermediary liability should be based on actual or constructive knowledge.
- There seems no certainty as to *when* that knowledge should be obtained in order to be relevant.
- There seems no certainty as to *how much positive action* (if any) an intermediary must take to avoid being deemed to have authorised an infringement by others; nor how far "*wilful blindness,*" eg allowing the use of encrypted files, will be deemed to be an evasion of actual knowledge, and the attendant obligations that knowledge would impose on the intermediary to block or remove infringing content.
- NTD regimes, in relation to decentralized P2P services of the post-Napster variety, are not helpful or relevant either to shield P2P intermediaries from liability, nor to provide them with guidance as to what to do to avoid facilitating copyright infringement by their users. Immunity depends on knowledge of infringing uses, and, importantly, the ability to stop those infringing uses at the time they occur or subsequently. Decentralised post-Napster services do not have that kind of control built into their architecture.
- The relevance of the extent of *potential or actual non infringing uses* of a technology to attribution of primary or secondary liability for copyright infringement has not been settled.
- Services such as BitTorrent, where files are transferred not as a whole but in chunks, and *where downloaders are also by default uploaders,* also present huge difficulties for concepts of knowledge, authorization, contributory liability and private copying exemptions.
- *Decentralised and anonymised* systems such as Freenet are likely to defeat any attempt to close them down as there is no one chokepoint of control nor a way to definitely identify users Such systems are currently difficult to use and therefore relatively unpopular but this is likely to change.
- *Open source systems* such as BitTorrent are also likely to be extremely difficult to close down as new clients can be built, modified and made available anywhere by persons other than the original author.

At its heart, this debate is as much about the regulation of technology as it is about copyright. What types of technologies should authors be permitted to develop and distributors to disseminate? Should the law interfere with technical design decisions and potentially impede effective

development of the technology? Technologies are, on the whole, value neutral and can be appropriated for good or bad ends: BitTorrent being a prime example.[177]

So what alternative ways forward might there be which would respect and enable the legitimate expectations of rightsholders to receive a fair return, but which would allow technology to develop without impeding legal interference?

Levies. Levy systems that compensate for private copying exist in a number of jurisdictions, and in recent years proposals have been made to extend such systems to P2P filesharing.[178] Could, or should a system of levies, whether on hardware, on software or on bits of traffic funneled through ISPs, be instituted to compensate content owners for sharing materials between individuals?[179] Such a solution might allow free technological development while at the same time providing content owners with a source of remuneration. Such proposals have so far been viewed with skepticism by the rightsholder industries and many academics. The institution of a system of levies, it is argued, would be inconsistent with the careful balancing act that is to be found within copyright legislation which takes cognisance of the interests not only of the content owners and the consuming public, but also the of existing and would-be authors;[180] it would turn copyright from a property right into a liability system where all users, no matter whether they used the software or hardware for infringing purposes, would pay for the acts of the minority. Yet others, such as William Fisher at the Berkman Center for Internet and Society take the attitude that if copyright is effectively unenforceable in the digital world, it is indeed better to move to a system of levies which protects the economic rights of renumeration of rightsholders (if not their moral rights) than to continue to apply laws which arguably no longer meet their purpose and which may restrain the development of key technologies.

Another forceful argument is that levies are not intended to compensate content owners for unlawful use.[181] Levies are currently collected on blank media (such as CDs) and recording hardware as a *quid pro quo* for lawful private copying by individuals, which is allowed in a majority of EC

---

[177] It is interesting to note that similar battles were fought in a very different Internet law context, namely, in regard to encryption. Encryption has "good" uses – enabling secure and integral transmission of commercial documents – but also has "bad" uses – allowing criminals and terrorists to communicate safely. In the end, control of "strong" encryption as a "dual use" technology was mostly abandoned in the US after the "Clipper Chip Wars" were fought and lost by the US; not least, and significantly for this paper, because US industry pled that if they were not allowed to export strong-encrypted products they would lose out in the European market to EC-made software that was allowed to integrate such encryption. One might imagine that a US technology industry where design decisions had to be licensed as non-invasive of copyright might well also fall behind industry players based elsewhere and not subject to such hypothetical regulation.

[178] Netanel N W "Impose a non commercial use levy to allow free P2P file swapping and re-mixing". University of Texas Public Law Research Paper, November 15, 2002.

[179] For a number of differing views on levies see generally *'Creators' Rights in the Information Society'*, collection of the Association Litteraire et Artistique (ALAI), Budapest 2003 (hereafter ALAI collection).

[180] Strowell A "C: C & C. Copyright: Control and Compensation", ALAI collection p. 309

[181] Hugenholtz P B, "The Future of Levies in a Digital Environment" available at http://www.ivir.nl.

Member States and in some other legal systems. It would of course be quite a different system that used levies to compensate the content industry for *unlawful* copying. The content industry might argue that their aim is to prevent illegal copying, not to be remunerated for it and in strict legal terms, they are so entitled. Levy systems would probably return a flat rate as opposed to what the market might bear. It is worth noting that the EC has in the past investigated evidence of price-fixing in relation to music CDs in Europe, where they retail at much higher prices than in the US. So a free market in music is not in any case guaranteed even without levies. Finally, there are administrative issues. Any widespread system of levies would surely require extensive regulatory oversight: to whom are the levies to be paid? What happens across borders? How can one be sure that the collecting societies (those who administer the levies) are acting in the best interests of their members? Such questions are already being addressed in relation to existing European and Canadian levy systems however, which operate to the satisfaction of many (if not all) of their stakeholders; it may be asked why existing levy structures could not accommodate the new systems. The EC is currently looking towards developing technological means of collecting and accounting for taxes, which will be essential to facilitate collection of VAT in a future Europe of virtual cross border trade.[182] It bears investigation whether software developed for VAT collection on virtual goods could be adapted for copyright levy collection on virtual downloads.

Digital rights management (DRM). The most pressing objection, perhaps, to levy schemes is that they will shortly be unnecessary when DRM systems regulate access to all content not in the public domain or being given away by the rightsholder. The Infosoc Directive[183], for instance, broadly contemplates that private copying levies will be phased out as digital rights management (DRM) systems increase in popularity.[184] And as use of DRM systems does gain popularity, a widespread system of levies would not only mean that those who do not copy pay for those who do, but also that those who use the DRM systems would pay twice[185]. Levies, it would seem, may not be the best short or long term answer to finding the balance between the interests of content owners and the need to allow technology freedom to develop. Instead, the use of DRM is the favoured option of the content industry: secure content and then bargain by contract for allowing access to buy, read or

[182] For a discussion see Basu S "Controlling information in the online environment. Implementing e-commerce tax policy" 18th Bileta conference April 2003 http://bileta.ac.uk/03papers/basu.html

[183] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001, on the harmonization of certain aspects of copyright and related rights in the information society.

[184] Ibid recital 39 and Articles 5.2(b) 6 and 7. Hugenholtz P B "The Future of Levies in a Digital Environment" in ALAI collection at pp 298-299.

[185] Some might argue that private copiers are *already* paying once for private copying by means of levies: DRM required payments merely replace the private copying levy. Therefore an additional levy to offset illegal copying would only represent one more burden, not two. It may also be said that levy systems such as suggested by Fisher spread the cost of both legal and illegal copying evenly on the basis that access to information and cultural goods is a public good: the model is more akin to a council or local authority tax used to provide free schools to everyone in the area, whether or not they have children, than to an extension of existing private copying levies.

listen and/or other types of rights (printing, burning, streaming, etc). To date, this model works best in the new online music systems such as iTunes and the new, legal Napster (see below). But there are clear difficulties in getting the technology right for all types of content in all media on all platforms (CDs, PCs, Macs, IPOds, mobile phones, etc.). Applying DRMs to all content is likely to be a long-term project, requiring complex contractual matrices among all those who need to be involved in its successful realization[186]. DRMs also raise issues which have arisen controversially in particular relation to the US DMCA, as to how user rights eg, of fair use or fair dealing, in copyright works, can be exercised when that content is secured by DRM.[187] Most of all, it is hard to have faith, given recent history, that the uncrackable DRM will ever really be here. Most consumers may not be skilled hackers of course, but in a world of P2P technologies, only a single skilled hacker is required for illegal non-DRM protected copies of a work to circulate at will.

Inducement. It has been suggested – in the context of the US Supreme Court's consideration of *Grokster* - that further analysis should be given to the 'active inducement theory' of liability: can P2P intermediaries be held liable on the basis that they actively induce others to infringe? There have been attempts, so far unsuccessful, to introduce such liability into US law by statute, such as notably the Inducing Infringement of Copyrights Act of 2004, introduced by Senator Orrin Hatch.

Join the club. If you can't beat 'em, join 'em, goes the saying, and one lateral answer to the problem of illegal downloading is not to sue P2P intermediaries, but to adopt their tactics within a legal, paying model. The prime example is Napster: having collapsed under the strain of its attempts to block infringing material, it has been reborn as a legal subscription site from which music files, protected by DRM technology to prevent illegal re-copying, can be downloaded or streamed for a fee.[188] Throughout Europe, iTunes and OD2 have also been extremely successful, using a similar legal paying model. In Korea, a majority shareholding in Bugs Music, an online music provider (although not a P2P intermediary in the sense discussed above), has been purchased by a local record company.[189] Successful legal streaming/download systems demonstrate that what illegal downloaders may have been looking for, more than just free music, may be the convenience, choice and diversity of the online model; and if this is provided with the additional benefit of no worries as to legality, users may be prepared to pay the relatively low fees required to use it. Napster, for example, currently costs only around £10 a month in the UK to access an enormous library of up to date and

[186] Perlmutter S, "Availability of Works, Choice for Consumers, Confidence in Markets", ALAI collection p. 283.
[187] See Waelde C and MacQueen H, "From Entertainment to Education: The Scope of Copyright?" [2004] IPQ 259, 278.
[188] See http://www.napster.com
[189] Bugs Music, Korea's largest online music provider, said recently that it plans to sell 60% of the company to local record companies to settle its lengthy copyright dispute with the music industry. "*We concluded that giving up our management control by selling more than half of the shares to recording companies is the only way for us to end the conflict with the local music industry and put the business back on track*," said Bugs Music Chief Executive Park Sung-hoon.at
http://www.koreaherald.co.kr/SITE/data/html_dir/2005/03/07/200503070016.asp.

back catalogue music, less than the cost of one CD. As a result, legal downloading increased tenfold in Europe and the US in 2004, and there is strong evidence in the UK at least that, in combination with fears as to litigation, illegal file-sharing has fallen as a result. Total music sales are also rising again: the number of CDs and other music products shipped from record labels to retail merchants rose 2 percent last year, to 814 million units, the first annual increase in five years, according to the RIAA. These trends may show that such business models may be the long term solution for resolving the content industries' problems with P2P.

Each of these alternatives deserves serious consideration and the fourth is already being actively pursued. But the most radical approach, and the one seemingly desired by the content industries, would be for the law to require developers to build systems that do not have infringing uses, or at least facilitate the prevention of such uses, eg, by disallowing encryption However, it is unlikely that the developers would relish the imposition of statutory technology mandates in their technical decision making processes; nor is it clear that jurisdictions such as the US would endorse the possible impacts on freedom of expression. We return to this point below.

K. Conclusions

The discussion above has described how the competing interests of the stakeholders in the Internet content industry – intermediaries, content providers, rights-holders, and the public interest or "users" - led at the turn of the millennium to creation of a "limited liability/notice and take-down" approach to online intermediary immunity. However, if it is accepted that the level and extent of ISP duties is a matter of balancing policy needs, and not simply a matter of historical accident, or natural justice, then it becomes plausible that as the Internet industry matures and policy interests change, so the imposition of ISP liability - or immunity from such - may also fluctuate. ISP immunity, as it was called when it began, was based on a perception of ISPs as beleaguered defendants, facing unlimited risk as a result of hosting or providing access to limitless amounts of content over which they had little or no control. This led to a need for immunities to safeguard the public interest in a healthy Internet access market. But since then, a number of factors have altered.

First, the balance between the interests of intermediaries and the rights of third parties affected by intermediary immunity – notably IP rightsholders – has had to be re-assessed in the light of the explosion of unlawful file-sharing using P2P networks. Second, the online intermediary industry has become more mainstreamed, and thus perhaps less in need of special protections to survive. Thirdly, the expectation that intermediaries would naturally be driven by market forces to remove and block illegal content has not altogether come to pass. Intermediaries left to their own devices do not see

content filtering as a core business activity, and will only largely remove illegal content on notice, both for fear of legal sanctions and as a matter of good public relations; but as we have seen, even NTD regimes are extremely problematic when considering the public interest and the public domain.

Fourthly, and most importantly a new class of intermediaries, the P2P intermediaries, have arrived which in some jurisdictions are seen by the law (and the content industries) as active accomplices to law-breaking rather than, as traditional ISPs have been, as friends of the public and neutral intermediaries. Yet if P2P services are now being specifically developed for, and used for, lawful purposes, such as sharing of public domain educational materials, or creative works with consent of the copyright owner, then this approach too may need reconsideration. Some form of immunity scheme for lawful P2P intermediaries may not only seem to be desirable but also essential if technological development is to continue. Yet given the essential value-neutrality of technologies, it is hard to see how a liability regime for "unlawful" and not "publicly beneficial" P2P intermediaries can be devised, except one wholly based on the intention of the service provider, such as the "active inducement" draft statutes we have seen introduced in the US. Interestingly, there has been a degree of emphasis on the "inducement" model in the oral arguments made by the record industries in *Grokster* in the US Supreme Court. Legislation solely based on intent, however, may be difficult to prosecute and enforce.

The content industry's preferred way forward, as noted above, is to require systems to be developed in ways that prohibit infringing uses. They suggest that ways should be found to monitor, track, and if necessary prohibit such usage, thus tailoring technological development to meet the needs of the content industry. Given the history of technology, such a managed, top-down, regulatory approach may negatively impact software development and hinder innovation.

Again, the Supreme Court in Grokster has, at the oral argument stage, also expressed concern at what the impact of such a choice might be. Justice Steven Breyer noted that many inventions, from the movable type printing press to the iPod digital music player, could be used to unlawfully copy protected works but have nonetheless proven beneficial to society. If inventors were uncertain if their products once developed would be legal, they would be disinclined to invent. "Licensed science" is also historically reviled for many reasons to do with distrust of central control, the need for lateral research, and freedom of academic and scientific expression. In particular the concept of a P2P technology is so wide - simple email can be seen as a P2P technology for example - and so easy to achieve – a working P2P system can be written in 18 lines of code – that any attempt to license 'approved systems' would in all likelihood be overwhelmed by the task of definition and

management (not to mention being largely unenforceable).

In the short to medium term, it is possible to predict that means of circumventing "traditional" intermediary immunity and neutrality which are already allowed under immunity instruments like the ECD and the DMCA - eg the seeking of injunctive relief[190], take-down/cease and desist letters, and demands to reveal the identity of anonymous or pseudonymous content providers - will be increasingly utilised by rightsholders against traditional hosts and ISPs. The content industries are also likely to continue to pursue a combined strategy of lawsuits against P2P intermediaries and individual users, alongside implementation of increasingly sophisticated DRM systems to protect content in various media. Simultaneously, they are likely to continue to explore new business models opened up, perhaps ironically, by the P2P sector. In the longer term, the biggest unknown is the extent to which any jurisdiction might require those who develop technology to include mechanisms to ensure that infringing content cannot be exchanged among users, or if it is, to build in the means whereby such uses can be identified and stopped. The forthcoming Supreme Court decision in *Grokster* may be a turning point in this debate, at least in the US. But even in the unlikely event that technology mandates were created, history shows that hackers have a way of getting around almost every software protection ever conceived. What one software writer can build, another can break. As content owners search for profitability in the Internet age, technological advance may hang in the balance. For online intermediaries generally, these are, in the Chinese sense, once again interesting times.

[190] Article 14(3).