article

Viral Online Copyright Infringement in the United States and the United Kingdom: the End of Music or Secondary Copyright Liability? (Part I)[1]

WARREN R. SHIELL[2]

"And why are you complaining? Everything you get out of our network is free. You could always do the legal thing, and go buy the game, we suppose?" (Grokster support email to user).

"An innovator has as enemies all the people who were doing well under the old order, and only half-hearted defenders in those who hope to profit from the new" (Niccolo Machiavelli).

Background

By the end of 2002, Kazaa, a supplier of peer-to-peer ("P2P") software that allows users to exchange music files over its FastTrack network, estimated that it had 140 million users. That's twice as many as Napster had at its peak. The International Federation of the Phonographic Industry (IFPI) estimated that online piracy was largely responsible for a 7 per cent drop in worldwide music sales in 2002. Against this background, the music industry in the United States has pursued an aggressive litigation strategy that has tested the limits of secondary copyright liability against the suppliers of P2P technology ("P2P providers") responsible for the explosion in online copyright infringement. Napster's shutdown has been well publicised even though damage claims remain outstanding. However, this early legal success proved to be short-lived as new P2P providers such as Kazaa, Grokster, Music City, BearShare and Limewire, to name a few, emerged to fill the void. In the winter of 2001, representatives of the motion picture studios and the record companies and a group of songwriters and music publishers filed two class action lawsuits against P2P providers, Kazaa BV, Grokster Ltd, and StreamCast Networks Inc. Because the new systems do not operate central servers like Napster they have proved more resilient to legal and technological challenges. In March 2003, District Court Judge Stephen V. Wilson granted Grokster and StreamCast's summary judgment motions in the consolidated class action ("the *Grokster* case").[3] Judge Wilson said that he would enter a default judgment against Kazaa, which had apparently ceased defending the action. The motion picture studios and recording industry have appealed and the outcome will have far-reaching consequences. The record industry has also begun suing individual users who download music aided by a favourable decision in *RIAA v Verizon Internet Services Inc*[4] (subsequently reversed), which upheld a subpoena compelling Verizon, an internet service provider ("ISP"), to disclose the identity of a Kazaa user who in a single day had downloaded more than 600 copyrighted songs. The Recording Industry Association of America ("RIAA") has taken out full-page adverts in major newspapers threatening to sue individuals who download their music and has started filing hundreds of lawsuits. A 2004 Online Music Report from the IFPI points to a decline in the use of some P2P networks as evidence that this strategy may, indeed, be working in the United States and elsewhere. On the legislative front, Senator Orrin Hatch, chair of the Senate Judiciary Committee, reflecting an earlier proposal of Representative Howard Berman, has gone on record saying that he would be in favour of technologies disabling the computers of illegal file-sharers, and there are other bills before Congress which would make the transfer of files over the internet without authorisation a criminal offence punishable by up to five years in prison and US$250,000 in fines.[5]

1. Part II of this article will be published in the next issue of *Entertainment Law Review*.
2. The Author would like to thank Professor Joseph Touch, University of Southern California Department of Computer Science, for his insights, and my wife for her support and encouragement.
3. Summary Judgment Order in *MGM Studios Inc v Grokster Ltd* (CV 01-08541); *Jerry Leiber v Consumer Empowerment* (CV 01-09923) 259 F.Supp.2d 1029 (C.D. Cal. 2003).
4. W.L. 141147 (D.D.C. 2003). rev'd RIAA Inc. v Verizon Inc., 351 F3d. 1229 (D.C. Circ., December 19, 2003). The result of the reversal will be that copyright holders will no longer be able to rely on the expedited procedures for issuing subpoenas under the Digital Millennium Copyright Act.
5. Proposed legislation to regulate emerging internet technologies includes H.R. 2885, 108th Cong. (2003) (regulate P2P software); H.R. ACCOPS 2752, 108th Cong. (2003) (criminal penalties for P2P sharing); H.R. 2517, 108th Cong. (2003) (criminal copyright enforcement); H.R. 5211, 107th Cong. (2002) (Berman Bill to disable P2P technology); S. 2048, 107th Cong. (2002) (mandated content-protection for software and devices).

By contrast, the United Kingdom has not yet entertained any P2P lawsuits despite the existence of a common law jurisprudence rooted in the concepts of authorisation and joint tortfeasance which are also the foundations of the US case law.[6] The only online music piracy case of note to reach the courts is *Sony Entertainment (UK) Ltd v Easyinternetcafé*, [7] shutting down the CD burning service of a chain of internet cafes. But that case merely restates the traditional English position regarding strict liability for copyright infringement. It remains to be seen whether the United Kingdom's Copyright and Related Rights Regulations of 2003 ("the Copyright Regulations"), Parliament's long-awaited implementation of the European Copyright Directive [8] (the European Union's equivalent of the Digital Millennium Copyright Act), will bolster the substantive laws in this field.

This article will review the legal frameworks which exist in the United States and United Kingdom for dealing with viral online infringement and ask what lessons can be learnt by UK policy-makers and courts from their American cousins.

The Technology

The threat to the music industry comes primarily from the widespread synergy of two technologies: P2P networking and MP3 compression technology. Briefly, MP3 (an abbreviation of Motion Picture Expert Group-1 Audio Layer 3) technology makes it possible to compress audio recordings in a digital format whereby an MP3 file may contain a fraction of the data of an uncompressed audio recording (approximately 12:1),[9] while P2P software allows computer users to connect directly with each other and exchange files.[10] It should be noted that advances in networking technology also threaten the film industry .[11]

MP3s

Consumers acquire MP3 files either from downloading them over the internet or by "ripping" CDs - that is the process of converting CDs into digital MP3s stored on a computer's hard drive. Regardless of whether you are part of a P2P network, the process of uploading and downloading MP3 files (and for that matter any files) to and from the internet is essentially the same. Once connected to the internet, a host computer breaks down, or "encapsulates", an MP3 file into thousands of data packets. Each data packet has a "header" which contains the Internet Protocol ("IP") address of the host computer and the IP address of the recipient's computer together with other information necessary to reassemble the packets upon arrival at their final destination. The internet can be viewed as a series of networks which use a basic set of communication protocols, commonly referred to as "TCP/IP", to facilitate the transfer of data packets between networks on the internet.[12] One of the most important protocols for sharing music is the "file share protocol"("FTP") which allows file-sharing between computers. Protocols can be compared to a language: some such as FastTrack are closed and proprietary and users can communicate with others using the same FastTrack language. Others such as Gnutella are open and can be built upon by software developers so that any programs incorporating Gnutella protocols may communicate with one another. ISPs such as America Online ("AOL") provide the hardware and routing equipment that allows individuals to connect to the internet. Routing of data packets constantly changes according to network demands and routing policies *(e.g.* the fastest route or least hops). When the data packets arrive at the destination IP address they are "reassembled" [13] into an exact copy of the MP3 file. In copyright terms, only one copy of a file is made when an MP3 is downloaded using the FTP protocol even though the parts of the MP3, the data packets, may be transmitted through several servers and networks.[14] The process is complicated by the fact that very few private individuals have permanent IP addresses, since most ISPs dynamically assign IP addresses to a user when they log on. This makes it very difficult for most personal computers to serve as hosts for storing and disseminating information. In 1999, a Northeastern University undergraduate named Shawn Fanning created a music file-sharing program called Napster which solved this problem for people who wanted to share MP3s.

P2P music programs

Napster

Napster's solution to the problem of dynamic IP addresses was to store on a central server a directory of continually updated IP addresses of Napster users together with the file names of MP3 files corresponding to those addresses. Each time a user logged on or off the Napster server using Music Share software, Napster's server would update the list of MP3 file names made available by that user on their hard drive in a "user directory". For this reason, Napster was referred to as a centralised model of P2P networking even though the actual MP3 files were stored on and transferred between

6. *See Harper v Shoppel.* 28 F613 (S.D.N.Y. 1886); *Kalem Co Harper Brothers*, 222 U.S. 55; 56 L.Ed. 92 (1911).
7. 2003 W.L 116984.
8. Directive 2001/29 of the European Parliament and of the Council of May 22, 2001, on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, O.J. L167/10.
9. Typically an uncompressed "wav file." A one-minute, 16-bit wav file at 44.1 kHz takes about 10MB of hard space and, using a telephone internet connection, about 40 minutes to download. Compression technology uses principles of psycho-acoustics to delete redundant audio information that cannot be perceived, *e.g.* louder sounds cover up softer ones when they occur simultaneously (frequency masking) or immediately before (temporal masking) See Tomlinson Holman, "Sound For Film and Television, Ch 2"
10. For a general overview, see Clay Shirky, "Listening to Napster" in *Peer-to-Peer Harnessing The Power of Disruptive Technologies* (Andy Oram ed. 2001)
11. Caltech has reported that they have developed a new data transfer protocol called "FAST" which allows a DVD movie to be downloaded in less than five seconds See *http: pr.caltech.edu media Press Releases PR 12356.html*
12. See Professor Lawrence Lessig's Expert Report to the court in the *Napster case* at *http cyberlaw.stanford.edu lessig content testimony nap napd3ldoc html*
13. Another term for reassembly is positive acknowledgement with retransmission("PAR")
14. The process of "proxy caching" whereby transient copies of files are stored on intermediary servers within the network in order to ease network traffic complicates this analysis. Niklas Zennstrom, who co-founded Kazaa, has developed a caching system for use with his FastTrack P2P protocol network, see "P2P Caching Unsafe at any Speed!", online at *http newscom.com 2102-1025-3-1027508.html*

end users' computers. Napster lost the lawsuits brought against it for copyright infringement in the Ninth Circuit in large part because of the role its central servers played in helping users locate infringing files.[15] This lesson was not lost on other P2P applications that emerged in the wake of Napster's demise. Some commentators have analysed the process in evolutionary terms, where the P2P programs most resilient to legal attack will survive.[16] These applications are similar to Napster[17] in that users copy files between their own computers: at no point are files copied or stored in a central computer operated by a software company. However, they differ in one critical respect: the companies that supply the application software do not operate central servers containing indexes of music file names and IP addresses. Learning from Napster, these companies have developed more decentralised networks by incorporating the search and indexing function into end users' personal computers. How they do this varies between applications.

Aimster/Madster[18]

Aimster software enhanced the functionality of AOL's Instant Messaging service allowing Aimster users to search for and download music files from the directories of other Aimster users who were simultaneously online. Aimster claimed it operated no central servers and the court was unable to determine conclusively whether Aimster maintained a central index of files.[19] Instead, the court focused on the role that ancillary services like tutorials, chat rooms and the ClubAimster service played in contributing to infringement.

Kazaa, Grokster and StreamCast[20]

Kazaa BV, formerly known as Consumer Empowerment BV, first developed FastTrack P2P technology and licensed it to Grokster Ltd, which distributed a branded version called Grokster, and to StreamCast Networks Inc, formerly called MusicCity.com Inc, which called its version Morpheus. Kazaa BV is now little more than a shell having transferred most of its assets to an offshore company, Sharman Networks Ltd, which also has the irrevocable worldwide license to use and distribute FastTrack.[21] A Grokster or Kazaa user who connects to the FastTrack network is directed to a "root supernode" which then directs them to other FastTrack users' computers temporarily designated by the software as indexes of available files and referred to as "local supernodes". A user's computer can automatically function as a local supernode one day and not another depending on that computer's processing power and the needs of the network. Grokster and StreamCast originally required users to log on to central servers with a username and a password but abandoned this practice shortly after they were sued. These supernodes are the functional equivalent of Napster's server except they are distributed throughout the network on individuals' computers. Only Sharman/Kazaa has access to FastTrack source code and can control the root supernodes.[22]

StreamCast's Morpheus software had originally employed FastTrack software but switched to open source Gnutella protocols following a payment licensing dispute with Kazaa. In order to join the network for the first time, the Morpheus software must obtain the IP address of at least one other user connected to the network, a process known as "bootstrapping". It does this by contacting a "host cache" maintained by third parties unrelated to StreamCast. At this point, search requests are passed from user to user in an exponentially expanding network until a match is found or the search request expires.[23]

Secondary Infringement in the United States

Proof of direct infringement

Any claim against a secondary infringer that supplies the means of infringement but does not necessarily carry out the infringement itself must first prove direct infringement by a third party.[24] This requires evidence of ownership of copyright material and proof that end users violated at least one of the five exclusive rights granted to copyright holders under 17 USC s.106.[25] In *Napster*, the first prong was satisfied by evidence presented to the District Court that up to 87 per cent of files on the defendants' servers were copyrighted and 70 per cent were owned by the plaintiffs. In *Grokster*, plaintiffs claim these figures were 90 per cent and 70 per cent. With regard to the second prong, the Ninth Circuit in *Napster* concluded that end users who downloaded MP3 files onto their computers violated copyright owners' reproduction rights,[26] and that users who uploaded file names to Napster's search index violated owners' distribution rights.[27] In *Napster*, the court rejected the defendants' arguments that end users were not direct infringers on the basis of the "fair use" exception in 17 USC s.107

15. On substantive issues, see *A&M Records Inc v Napster Inc*, 114 F.Supp.2d 896 (N.D. Cal. 2000); affirmed in part by *A&M Records Inc v Napster Inc*, 239 F.3d 1004 (9th Cir. 2001). On the scope of the preliminary injunction, see *A&M Records Inc v Napster Inc*, 2001 W.L 227083 (N.D. Cal. March 5, 2001); *A&M Records Inc v Napster Inc*, 284 F.3d 1091 (9th Cir. 2002).
16. See Andrew Frank, "The Copyright Crusade."
17. Actually, they are broader: Napster only allowed the downloading of MP3s whereas Grokster and Morpheus cater to all types of computer files.
18. In *Re Aimster Copyright Litigation* 2003 W.L. 21488143 (7th Cir. 2003) affirming *Aimster Copyright Litigation, Re*, 252 F.Supp.2d 634.
19. *Aimster*, 252 F.Supp.2d 634 at 642.
20. Facts relied on to describe these systems borrow heavily from the briefs submitted in the *Grokster* litigation and are highly contested. Key declarations regarding technical specifications of the systems (*e.g.* Professor Kleinrock's) are under seal and not available to the public.
21. The FastTrack software is apparently owned by Joltid Ltd, which is owned by Niklas Zennstrom who launched Kazaa BV. Sharman Networks Ltd is registered in the South Pacific Island of Vanuata with Australia as its principal place of business. For more details, see Order Denying Defendant Sharman Networks Ltd and Defendant LEF Interactive's Motion to Dismiss, 243 F.Supp.2d 1073 (C.D. Cal. 2003).
22. *Grokster*, 259 F.Supp.2d at 1040, n.6.
23. To preserve internet bandwidth, most Gnuttela requests are limited by "time-to-live" ("TTL") constraints that limit the number of sites that can be searched. Generally, see Gene Kan, "Gnutella" in *Peer-to-Peer: Harnessing: The Power of Disruptive Technologies* (Andy Oram ed., 2001).
24. *Sony Corp of America v Universal Studios, Inc* 104 S.Ct. 774.
25. *Napster*, 239 F.3d 1013.
26. s.106(1), to reproduce the copyrighted work in copies or phonorecords.
27. s.106(3), to distribute copies of phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease or lending.

and the "home taping" protections afforded by 17 USC s.1008 of the Audio Home Recording Act of 1992.

Audio Home Recording Act 1992

This Act was enacted to protect the right of consumers to "make analog or digital audio recordings of copyrighted music for their private, non-commercial use".[28] Section 1008 of the Act provides immunity for the non-commercial use by a consumer of a "digital audio recording device" for making "digital musical recordings or analog musical recordings". However, such "digital audio recording devices" must meet the requirements of the Serial Copyright Management System ("SCMS"), which allows unlimited first-generation copies of an original source but prohibits second-generation copies[29] (copies of copies) and provides for the payment of royalties.[30] The Ninth Circuit in *Napster* followed their earlier ruling in *Recording Industry Association of America v Diamond Multi Media Systems, Inc*[31] which held that users were not protected by the Act because computers did not fall within the statutory definition of "digital audio recording device".[32] The Act defines a "digital musical recording" as a "material object (i) in which are fixed, in a digital format, only sounds, and material, statements, or instructions incidental to those fixed sounds, if any",[33] but does not include "a material object (ii) in which one or more computer programs are fixed".[34] In the court's view, once an MP3 is copied onto the hard drive of a computer it ceases to be a "digital music recording" for the purposes of the Act because a computer's primary purpose is not to make digital audio recordings. In the *Diamond* case, the court applied the same logic to exempt from the SCMS requirements of the Act the manufacturers of the Rio, a portable device with headphones which enabled users to download MP3s from their computer hard drives.

The "fair use" exception: 17 USC s.107

Section 107 of the Copyright Act provides the following list of non-exhaustive factors for courts to consider in determining whether a use is fair:

> 1. the purpose and character of the use, including whether such use is of a commercial nature or is for non-profit educational purposes;
> 2. the nature of the copyrighted work;
> 3. the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
> 4. the effect of the use upon the potential market for a value of the copyrighted work.

With regard to the first factor (purpose and character), the Ninth Circuit in *Napster* found that downloading MP3s was not "transformative" and therefore did not add a different purpose or character to the work. Furthermore, the sending of files to anonymous end users combined with the fact that users got for free something they would otherwise have to buy rendered the unauthorised copying a commercial use. The court found the second factor (nature of the copyrighted work) weighed against fair use because the musical recordings being copied were creative in nature, as did the third factor (substantiality of the work copied), because users copied entire works. Lastly, unauthorised copying by Napster users harmed the plaintiff's existing and potential markets for its work by reducing the sale of CDs among college students and by creating barriers to the plaintiff's entry into the digital downloading market—in other words, who would pay for something they could get for free?[35]

The Ninth Circuit affirmed the District Court's rejection of Napster's arguments that users who "sampled" or used Napster for "space-shifting" purposes were engaging in a fair use. The sampling argument is one that is frequently put forward by users of P2P music networks. The argument is that users download MP3s to "sample" music to help them decide whether to purchase CDs. The District Court agreed with the plaintiff's experts that this simply was not the case: the evidence showed that music sampling actually led to a decrease in sales[36] and inhibited the plaintiff's efforts to develop their own digital download market.[37] Affirming, the Ninth Circuit noted that even if the evidence showed that sampling had a positive effect on CD sales, as a matter of law the "fair use" analysis would still require protection of the copyright holders' right to license material.[38] The court cited an example used by the Supreme Court in *Campbell v Acuff-Rose Music, Inc*,[39] that an unlicensed use of a previously unknown song in a film that turns the song into a commercial success would not make the song's copying fair.

Secondly, the defendants argued that downloading MP3 files to listen to music users already owned on CD constituted non-commercial "space-shifting". The Ninth Circuit distinguished *Diamond* (fair use to make copies on a portable device of recordings already residing on a user's hard drive for personal use)[40] and *Betamax* (fair use for someone to videotape a TV broadcast for later home use)[41] because time-shifting in those cases only exposed copyrighted material to the original user whereas a Napster user who lists a copy of a song he already owns in order to access it from another location exposes the song to "millions of other individuals".[42]

Proof of secondary infringement

Sony Corp of America v Universal Studios, Inc[43]

Although it is sometimes referred to as the *Betamax Defence*, this landmark Supreme Court decision remains the cornerstone of secondary copyright liability. In a five-to-four ruling, the Supreme Court sought to strike a balance between the rights of copyright holders and the needs of society in encouraging technology innovation by holding that the defendant manufacturers of Betamax video tape recorders were not liable for contributory

28. Senate Report 102-294 (1992) at *86.
29. s.1002.
30. s.1003.
31. 180 F.3d 1072 at 1078 (9th Cir. 1999).
32. *Napster*, 239 F.3d at 1024.
33. s.1001(1).
34. s.1001(5)(B).
35. *Napster*, 239 F.3d at 1015–1016.
36. *Napster*, 114 F.Supp.2d at 915, citing the Jay Rep. at 4, 21 and Table 7.
37. *Ibid.* at 913.
38. *Napster*, 239 F.3d at 1018.
39. 510 U.S. at 591, n.21, 114 S.Ct. 1164.
40. *Diamond*, 180 F.3d 1072.
41. *Sony*, 104 S.Ct. at 782–785.
42. *Napster*, 239 F.3d at 1019.
43. *Sony*, 104 S.Ct. 774.

infringement because VCRs were "capable of commercially significant non-infringing uses", namely time-shifting of TV broadcasts.[44]

The entire court, however, agreed that secondary infringement ("the imposition of liability for copyright infringements on certain parties who have not themselves engaged in the infringing activity") was a recognised principle of law in spite of the absence of specific statutory language:

> "[t]he label 'contributory' infringement has been applied in a number of lower court copyright cases involving an ongoing relationship between the direct infringer and the contributory infringer at the time the infringing conduct occurred. In such cases, as in other situations in which the imposition of vicarious liability is manifestly just, the 'contributory' infringer was in a position to control the use of copyrighted works by others and had authorized the use without the permission from the copyright owner."[45]

The majority contrasted a number of authorities (the so-called *Dance-hall Cases*)[46] imposing liability on concert promoters and managers who had control over the use of copyrighted material with the *Landlord–Tenant Cases* in which landlords who leased premises to a direct infringer for a fixed rental and did not participate in any infringement were not liable for contributory infringement.[47]

The majority held that a seller of an article of commerce that was capable of commercially significant non-infringing uses could not be liable for contributory infringement because that would require a finding that the supplier had constructive knowledge that the article would be used for infringement.[48] However, the court was divided on the degree of proof required for a showing that an article was capable of significant commercial non-infringing uses. The minority favoured a factual analysis comparing current infringing and non-infringing uses:

> "If a significant portion of the product's use is non-infringing, the manufacturers and sellers cannot be held contributory liable ... [I]f virtually all the product's use, however, is to infringe, contributory liability may be imposed."[49]

While the majority rejected a current use analysis, it nevertheless considered in some detail evidence presented to the District Court regarding the existing use of VCRs for non-infringing time-shifting purposes:

> "The question is thus whether the Betamax is capable of commercially significant non-infringing uses ... [W]e need only consider whether on the basis of the facts as found by the District Court a significant number of them would be infringing. Moreover, in order to resolve this case we need not give precise content to the question of how much use is commercially significant."[50]

Whether proof of current non-infringing uses is a condition or merely one of many factors a court may consider in answering this question is one that has divided the courts in the P2P cases. The Ninth Circuit in *Napster* stated that

> "the District Court improperly confined the use analysis to current uses, ignoring the system's capabilities ... [C]onsequently, the District Court placed undue weight on the proportion of current infringing use as compared to current and future non-infringing use."[51]

The court cited a Fifth Circuit case, *Vault Corp v Quaid Software Ltd*, in which a single non-infringing use had implicated *Sony*.[52] In *Aimster*, the District Court could not find any evidence that the Aimster software had been used for any non-infringing purposes.[53] The Seventh Circuit refused to accept the defendant's argument that Aimster software was capable of substantial non-infringing uses simply because the software might or could be used for non-infringing purposes: "[w]ere that the law, the seller of a product or service used solely to facilitate copyright infringement, though it was capable in principle of non-infringing uses, would be immune from liability".[54] However, without citing any authority, Judge Posner attempted to read into *Sony* a cost-benefit test:

> "Even where there are non-infringing uses of an internet file-sharing service, moreover, if the infringing uses are substantial then to avoid liability as a contributory infringer the provider of the service must show that it would have been disproportionately costly for him to eliminate or at least reduce substantially the infringing uses."[55]

Since there was no finding of any non-infringing uses in *Aimster*, Judge Posner's test should be regarded as mere dictum. It can be argued that such a test would have a chilling effect on technology development if engineers had to second-guess the copyright consequences of designing products that might be used to facilitate copyright infringement.

Contributory infringement

Although *Sony* used the terms "contributory liability" and "vicarious liability" interchangeably, the cases cited by the court reveal two distinct theories which have been further refined by the courts, particularly the Ninth Circuit, in dealing with online copyright infringement. The major difference is that vicarious liability does not require actual knowledge by the infringer of the infringing activity.

The classic statement of the doctrine of contributory infringement, quoted in both *Napster* and *Grokster*, is: "One who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing activity of another, may

44. *Ibid.* at 789.
45. *Ibid.* at 786.
46. *Ibid.* at 786, citing *Famous Music Corp v Bay State Harness Horse Racing and Breeding Association*, 554 F.2d 1213 (CA1 1977); *KECA MUSIC, Inc v Dingus McGee's Co*, 432 F.Supp. 72 (W.D. Mo. 1977); *Dreamland Ball Room v Shapiro, Bernstein & Co*, 36 F.2d 354 (CA7 1929).
47. *Sony*, 104 S.Ct. at 787, citing *Deutsch v Arnold*, 98 F.2d 686 (CA2 1938).
48. *Sony*, 104 S.Ct. at 787.
49. *Ibid.* at 814.
50. *Ibid.* at 787.
51. *Napster*, 239 F.3d at 1021. The District Court considered an expert report that only 1 per cent of MP3s randomly selected on the network had been listed in the defendants' non-infringing New Artists service. See *Napster*, 114 F.Supp. at 904.
52. 847 F.2d 255 at 264–267 (5th Cir. 1988).
53. *Aimster*, 252 F.Supp.2d at 653.
54. *Aimster*, 2003 W.L. 21488143 at 7.
55. *Ibid.* at 10.

be liable as a contributory infringer."[56] It has been described as an outgrowth of enterprise liability and the common law doctrine that one who knowingly participates in or furthers a tortious act is liable as a joint tortfeasor.[57]

Knowledge

Although the courts generally agree with the proposition that liability requires that a contributory infringer either "knows or has reason to know" of the infringing activity, there is some disagreement when it comes to applying that definition to P2P technology.[58] P2P developers argue that *Sony*'s rejection of constructive knowledge requires actual knowledge of specific acts of infringement, whereas plaintiff copyright holders would like to see P2P providers held liable if they are generally aware that their systems/networks are being used to infringe.[59] In *Napster*, the Ninth Circuit distinguished the District Court and referred to Napster's actual knowledge of specific acts of infringement without expressly ruling against the District Court's finding that constructive knowledge would have sufficed. The court characterised the 12,000 RIAA copyright notices of infringing files on users' computers and a document authored by the co-founder of Napster, Sean Parker, on the "need to remain ignorant of users' real names and IP addresses since they are exchanging pirated music" as "actual, specific knowledge of direct infringement".[60] The court rejected the defendant's arguments that it could not have actual knowledge of infringing activity because in all cases where it had received RIAA notices it had terminated user accounts, and that it could not distinguish between infringing and non-infringing content on the basis of file name alone.[61] In other words, once the defendant became aware of infringing activity on its network in the form of MP3 file names listed on its server, the defendant was presumed to have actual notice of all copies of that song—present and future—on the network. Whether one views this as actual notice or a narrow form of constructive notice, as some commentators have suggested,[62] it is difficult to confuse it with the general type of constructive knowledge that was rejected in *Sony*. For example, if Sony had had "actual specific knowledge" that particular purchasers intended to use the Betamax recorders to make infringing copies, the court, no doubt, would have found Sony liable. The *Sony* court suggested one situation where this might hold: where the supply of an article must necessarily result in infringement.[63] In all other cases, it is submitted that *Sony* stands for the proposition that where a product can be used for both infringing and non-infringing purposes, one can generally only have actual knowledge of infringing activity where the supplier maintains an ongoing relationship with the user and can control its use ("the contributory infringer was in a position to control the use of the copyrighted work by others and authorized its use").

Much of the disagreement regarding actual versus constructive knowledge, in fact, stems from a failure to distinguish at the outset between the supply of a product and the continuing provision of a service, such as an integrated computer network, where the provider maintains an ongoing relationship with users and retains some degree of control. This basic distinction underscores the *Napster* court's rationale for distinguishing *Sony*. Drawing upon its earlier analysis in *Netcom*, the Ninth Circuit distinguished between the design of Napster's system and Napster's conduct in relation to its operation:

> "[I]f a computer system operator learns of specific infringing material on his system and fails to purge such material from the system, the operator knows of and contributes to direct infringement. Conversely, absent any specific information which identifies infringing activity, a computer system operator cannot be liable for contributory infringement merely because the structure of the system allows for the exchange of copyrighted material."[64]

However, the *Grokster* court found that the defendants, Groskter and StreamCast, were not liable because when they received notices of specific infringement from the RIAA they had no control over the network and were therefore unable to purge the system of infringing material:

> "[I]n order to be liable under a theory of contributory infringement, they must have actual knowledge of infringement at a time when they can use that knowledge to stop the particular infringement."[65]

The court applied *Netcom* which distinguished the *Landlord–Tenant Cases* cited in *Sony* where the landlord's liability for contributory infringement was contingent upon knowledge at the time of signing the lease that the premises were to be used for infringement.[66]

56. Citing *Gershwin Publishing Corp v Columbia Artists Management, Inc*, 443 F.2d 1159 at 1162 (2nd Cir. 1971).
57. 3 Nimmer s.1204[a][2] at 1275 and 1 Niel Borstyn on Copyright s.10.06[2] at 10–21 cited with approval in *Fonovisa, Inc v Cherry Auction, Inc*, 76 F.3d 259 (9th Cir. 1996).
58. *Napster*, 114 F.Supp.2d at 918; *Napster*, 239 F.3d at 1020, citing *Cable/Home Communication Corp v Network Productions, Inc*, 902 F.2d 829, and *Religious Technology Center v Netcom On-Line Communication Services, Inc*, 907 F.Supp. 1361 at 1373–1374 (N.D. Cal. 1995); *Aimster*, 252 F.Supp.2d at 649.
59. Generally, see MGM Plaintiffs-Appellants' Opening Brief to the Ninth Circuit in *Grokster* at 27–32, available online at *www.eff.org*.
60. *Napster*, 239 F.3d at 1021. Accordingly, the Circuit court found it unnecessary to explicitly reject the District Court's finding that constructive knowledge was sufficient based upon the facts that (a) Napster executives had recording industry experience; (b) they have enforced intellectual property rights in other instances; (c) Napster executives have downloaded copyrighted songs from the system; and (d) they have promoted the site with "screen shots listing infringing files": *Napster*, 114 F.Supp.2d at 917.
61. The court drew upon *Netcom*, 907 F.Supp. at 1373, which held that in order to hold a bulletin board operator liable for the posting of copyrighted material, the copyrighted material must "provide the necessary documentation to show there is likely infringement".
62. See David L. Hayes, "Copyright Liability of Online Service Providers: Part I", *Computer and Internet Lawyer*, October 2002. This is also the position adopted by the Plaintiffs-Appellants in the *Grokster* appeal.
63. Citing *Kalem Co v Harper Brothers*, 222 U.S. 55; 32 S.Ct. 20.
64. *Napster*, 239 F.3d at 1021, citing *Sony*, 104 S.Ct. 774.
65. *Kazaa*, 259 F.Supp.2d at 1037.
66. *Netcom*, 907 F.Supp. at 1373, distinguishing *Deutsch v Arnold*, 98 F.2d 686 at 688 (2d Cir. 1938). In contrast to the landlord in *Deutsch*, Netcom retained some control over the use of its premises, *i.e.* the system. Thus, the relevant time

The plaintiffs have argued on appeal that this finding is without precedent and incorrectly imports the notion of control into contributory infringement.[67] It is submitted that control is a relevant factor because it defines the scope of the "infringing activity" and therefore the time frame during which an infringer may acquire knowledge. In *Sony*, the "infringing activity" occurred after the sale and the court would not impute knowledge (constructive knowledge) because Sony had no control over its product's use. In *Napster*, the "infringing activity" which Napster knew or had reason to know about took place on its network evidenced by the listing of illegal file names on Napster's server. By contrast, the District Court in *Grokster* without explanation treated Grokster and StreamCast as suppliers of software (an article in *Sony* terms) as opposed to the operator of an integrated network or system (in *Napster* terms). As we will see in the discussion of the material contribution prong, the key issue underlying the District Court's decision is not whether control is a factor but whether the required degree of control must be a present ability to prevent infringement.

In *Aimster*, the District Court took the position that Aimster's "ongoing relationship" with users, in the form of chat rooms and bulletin boards, defined the boundaries of its knowledge of "infringing activities" without any finding that it had any "control" over its network. The District Court found that Aimster knew or should have known of the infringing activity on its system by reason of its receipt of cease and desist letters from the RIAA and Aimster's operation of chat rooms and bulletin boards in which users openly discussed infringement.[68] The Seventh Circuit took a more circumspect view that "the ability of a service provider to prevent its customers from infringing is a factor to be considered in determining whether the provider is a contributory infringer ... [i]t is not necessarily a controlling factor".[69] However, it did not have to decide the issue because it imputed knowledge to Aimster based on its attempt to hide behind its software's encryption features: "Willful blindness is knowledge, in copyright law (where indeed it may be enough that the defendant should have known of the direct infringement)."[70] The plaintiffs raise this argument for the first time in the *Grokster* appeal—namely that the defendants designed and operate their systems with features such as encryption of data and outsourcing of search functions (supernodes) to personal computers to cloak themselves in "willful blindness".[71]

Material contribution

In an online context, courts have drawn upon the Ninth Circuit's decision in *Fonovisa, Inc v Cherry Auction* that "providing the site and facilities for known infringing activities is sufficient to establish contributory liability".[72] In that case the defendant provided the "site and facilities" for a swap meet for counterfeit goods by renting out space, providing support services such as utilities, parking, advertising and plumbing, and attracting customers. The courts in *Napster* and *Grokster* reached opposite conclusions based upon the degree to which the defendants in each case provided the "site and facilities" for widespread infringement. In *Napster*, the court found that its software and servers facilitated users locating and downloading files. In *Grokster*, Judge Wilson framed the "critical question" as "whether Grokster and StreamCast do anything, aside from distributing software—or whether they could do anything—to stop their users infringing activities".[73] The court determined that the current versions of Grokster/Morpheus software merely allowed users to connect to their respective networks and search for and exchange files without any material involvement of the defendants. For example, Grokster had no control over supernodes and StreamCast had dispensed with them altogether when it switched to the Gnutella network. This meant that "if either defendant closed their doors and deactivated all computers within their control, users of their products could continue sharing files with little or no interruption",[74] whereas when the Napster site was deactivated, the entire network shut down. The court then rejected as proof of defendants' material contribution to infringement a number of technical support emails, un-moderated chat room conversations between users discussing copyrighted files, and the offer of software modifications and upgrades, since such contacts were not related to the underlying infringement, *i.e.* they did not facilitate or contribute to the exchange of files.[75] The court compared such incidental support services and refinements to those offered by companies like Sony or Xerox after the sale of their products. The court did not address the plaintiffs' other arguments that the defendants had at various times blocked users from the networks and continually maintained the integrity and performance of the networks.[76] The plaintiffs-appellants argue that the District Court misapplied the "material contribution" test claiming that the Ninth Circuit in *Fonovisa* explicitly rejected the District Court's importation of control into the concept of material contribution:

> "The district court apparently took the view that contribution to infringement should be limited to circumstances in which the defendant 'expressly promoted or encouraged the sale of counterfeit products or in some manner protected the identity of the infringers' (847 F.Supp. 1492 at 1496). We agree with the Third Circuit's analysis ... that providing the site and facilities for known infringing activity is sufficient to establish contributory liability."[77]

While this certainly supports the plaintiffs' argument that control does not have to extend to controlling the behaviour of particular

frame for knowledge was not when Netcom signed an agreement with the operator of a bulletin board but when it provided ongoing Internet services to the infringer.

67. MGM Plaintiffs-Appellants' Opening Brief to the Ninth Circuit in *Grokster* at 32–33.
68. *Aimster*, 252 F.Supp.2d at 659.
69. *Aimster*, 2003 W.L. 21488143 at 4.
70. *Fonovisa*, 259 F.Supp.2d at 1041.
71. Leiber Plaintiffs-Appellants' Opening Brief to the Ninth Circuit at 14–16.
72. Id. at 264, cited in *Netcom*, 907 F.Supp. at 1372; *Napster*, 239 F.3d at 1022.
73. *Grokster*, 259 F.Supp.2d at 1039.
74. *Ibid.* at 1041.
75. *Ibid.* at 1042.
76. MGM Plaintiffs' Brief to the District Court in *Grokster* at 11–16, 20–23.
77. *Fonovisa*, 76 F.3d at 264.

infringers, it does not entirely dispense with the issue of control, since one cannot be said to have a "site" without exerting some degree of control. In other words, we are back to the initial framing issue as to whether one is dealing with the supply of an article (a software program) or the operation of an integrated communications network (the cyber equivalent of a swap meet).

The Seventh Circuit in *Aimster* sidestepped the issue altogether; distinguishing *Sony*, it held that the provision of services like the Aimster tutorial instructing users how to download files using as examples only copyrighted files covered by the RIAA copyright notices was an "invitation to infringement".[78] The plaintiffs in the *Grokster* appeal raise a similar point by drawing the court's attention to the defendants' advertising material which featured copyrighted songs.[79]

Vicarious liability

A person is vicariously liable if he has "the right and ability to supervise the infringing activity and also has a direct financial interest in such activities".[80] *Sony*'s "staple article of commerce" analysis has been held inapplicable to vicarious liability and one can be liable without knowledge of infringement.[81]

Financial interest

This has been held to include future or speculative financial benefit. In *Napster*, it was the exponential increase in users which Napster could leverage to raise revenue.[82] In *Grokster*, the court looked to advertising revenues coming from pop-up advertising tags embedded in the software.[83]

Right and ability to supervise

In *Napster*, the Ninth Circuit pointed to Napster's reservation of rights policy[84] together with the ability to block users' access to the network (which it frequently exercised) as "evidence of the right and ability to supervise" its system.[85] The court stated that in order to avoid liability, the "reserved right to police the system must be exercised to its fullest extent", which Napster had the ability to do because it could carry out searches of its central index for copyrighted materials by file name.[86] The Ninth Circuit held that the District Court's initial preliminary injunction was overbroad because Napster's "right and ability" to police its system was "cabined by the system's current architecture", which at the time of the injunction was limited to a text-based filter to block copyrighted works noticed by the plaintiffs.[87] However, this proved to be less than 100 per cent effective as users deliberately mis-spelt file names. Napster's subsequent adoption of a content-based filter using audio fingerprinting technology also proved to be problematic. After several legal challenges to the preliminary injunction and modifications, the Ninth Circuit finally upheld the District Court's order shutting down Napster for lack of compliance.[88]

In *Aimster*, the District Court also found the defendant vicariously liable based upon a reservation of rights policy and ability to terminate user accounts. However, this is more sweeping than *Napster* and *Fonovisa*, since Aimster did not have the ability to "patrol" its premises as all communications were encrypted and there was no central directory of files that could be searched.[89] The Seventh Circuit declined to consider the issue of vicarious liability because it had already decided that Aimster was liable for contributory infringement.

The District Court in *Grokster*, however, accepted the defendants' arguments that they did not have the right nor ability to supervise:

> "Defendants provide software that communicates across networks that are entirely outside Defendants' control. In the case of Grokster, the network is the proprietary FastTrack network, which is clearly not controlled by Defendant Groskter. In the case of StreamCast, the network is Gnutella, the open source nature of which apparently places it outside the control of any single entity."[90]

Plaintiffs argue on appeal that this misapplies the *Fonovisa* test and urge the court to look at the quality of the defendants' participation in the infringement.[91] In *Fonovisa*, the Ninth Circuit rejected the District Court's holding that the right and ability to supervise relates to control of the sale of infringing records[92] and instead looked to the defendant's "pervasive participation in the formation and direction of the direct infringers, including promoting them (*i.e.* creating an audience for them)".[93] However, the

78. *Aimster*, 2003 W.L. 21488143 at 8.
79. Leiber Plaintiffs' Opening Brief to the Ninth Circuit in the Kazaa appeal at 14–16.
80. *Napster*, 239 F.3d at 1021, citing *Fonovisa*, 76 F.3d at 262. See *Gershwin*, 443 F.2d at 1162.
81. *Napster*, 239 F.3d at 1022; see also *Adobe Systems, Inc v Canus Productions, Inc*, 173 F.Supp.2d at 1049.
82. *Napster*, 239 F.3d at 1023, citing *Fonovisa*, 76 F.3d at 263–264.
83. *Grokster*, 259 F.Supp.2d 1044 at p.29. For Kazaa, presently estimated at US$450,000 per week.
84. The policy on its website reserved the "right to refuse service and terminate accounts in [its] discretion, including but not limited to, if Napster believes the user violates applicable law ... or for any reason in Napster's sole discretion, with or without cause".
85. *Napster*, 239 F.3d at 1023, citing *Fonovisa*, 76 F.3d at 262.
86. *Napster*, 239 F.3d at 1023–1024.
87. *ibid.* at 1027.
88. *Napster*, 284 F.3d 1091, affirming District Court's modified preliminary injunction in 2001 W.L. 227083; 2001 W.L. 777005; 2001 W.L. 789461.
89. *Aimster*, 252 F.Supp.2d at 655.
90. *Grokster*, 259 F.Supp.2d at 1045.
91. See MGM Plaintiffs' Opening Brief to the Ninth Circuit in the Kazaa appeal at 54–56.
92. "The argument that defendants could have 'policed' the vendors by refusing to lease spaces to them only has specious appeal. For one thing, the *Shapiro* court speaks of a priori supervisory power; that is, the power to supervise the direct infringers in the general course of business, e.g., what to sell, who to hire, how much to charge. Defendants could not inferably have assumed this supervisory role over the vendors": *Fonovisa*, 847 F.Supp. 1492 (E.D. Cal. 1994).
93. Citing *Gershwin*, 443 F.2d at 1163: "In Gershwin, the defendant lacked the formal contractual ability to control the direct infringer. Nevertheless, because of the defendant's 'pervasive participation in the formation and direction' of the direct infringers, including promoting them (*i.e.* creating an audience for them), the court found the defendants were in a position to police the direct infringers and held that the control element was satisfied."

court also said that the key element was the ability to terminate the vendors at the swap meets:

> "Cherry Auction had the right to terminate vendors for any reason whatsoever and through that right had the ability to control the activities of vendors on the premises. In addition, Cherry Auction promoted the swap meet and controlled the access of customers to the swap meet area."[94]

Does this mean that an operator must have the right and ability to block access to the network before it can be held vicariously liable, or can the right and ability to supervise be satisfied with some lesser control, *e.g.* ability to filter out unwanted material such as pornography, or maintain the integrity and performance of the networks by optional and automatic upgrades?[95] Plaintiffs argue that the best evidence that the defendants have the ability to supervise their networks is the fact that they jettisoned that ability when they realised that earlier versions of their software (which required user passwords and allowed for control over supernodes) might expose them to legal liability.[96]

Digital Millennium Copyright Act safe harbours

The Digital Millennium Copyright Act ("DMCA"), 17 USC s.512, provides a set of four safe harbours that online service providers ("OSPs") can raise as an affirmative defence to a claim for monetary damages and injunctive relief. These are the s.512(a) transitory communications, s.512(b) systems caching, s.512(c) innocent storage and s.512(d) information tools safe harbours. In *Napster* and *Aimster*, the courts considered s.512(a),(b),(d). The courts broadly interpreted the definition of OSP in s.512(k)(1)(A)[97] and s.512(k)(1)(B)[98] to cover the Napster and Aimster services even though neither would probably be considered an ISP as the term is commonly understood. In *Aimster*, the court rejected the defendant's argument that the service was primarily a location tool and did not provide routing connections to the internet. It was enough that these connections were provided by other intermediate service providers with which the defendant maintained contractual relationships.

As a threshold matter, the District Courts in *Aimster* and *Napster* held that the defendants could not satisfy the provisions of s.512(i)(1)(A) that first require an OSP claiming the protections of the safe harbours to show that it has

> "adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers."

In dismissing Napster's motion for a summary judgment, the District Court was unimpressed by the fact that Napster had implemented a policy of blocking infringing users' accounts since such users could simply log on using another account name. The plaintiffs argued that Napster would have to show that it permanently blocked IP addresses of offending users. How they would have done this for the majority of users with dynamic IP addresses remains unclear.[99] The Seventh Circuit in *Aimster* agreed with the District Court's interpretation of s.512(i) and ended further discussion of the DMCA safe harbours. The Ninth Circuit in *Napster* said that the issue would have to be resolved at trial. However, each of the District Courts considered the applicability of the DMCA safe harbours.

Both *Aimster* and *Napster* District Courts agreed that s.512(a) (transitory communications safe harbour) was inapplicable because the transmission of MP3 files between users passed through the internet and not the defendants' servers and was therefore not a transmission "through a system or network controlled or operated by or for the service provider".[1] The *Aimster* court regarded s.512(b) (caching safe harbour) inapplicable for the same reason. In addition, the Aimster system encrypted messages between users and therefore any material cached on the system had been modified, thereby taking it outside the scope of s.512(b)(2)(A). The court also made the obvious point that the safe harbour was designed to protect OSPs whose liability arose "by reason of the intermediate and temporary storage of material". Aimster's liability arose from its acts of contributory infringement and it could not hide in the safe harbour just because that material may have been cached on its system or network.[2] Lastly, both *Aimster* and *Napster* rejected arguments that their services were entitled to the s.512(d) safe harbour as information location tools because they had actual or constructive knowledge of infringing activities in violation of s.512(d)(1)(A) and (B). The *Aimster* court also pointed out that the defendants fell foul of s.512(d)(1)(D) by not taking steps to remove or disable access to infringing material and s.512(d)(2) by receiving a financial benefit directly from the infringing activity.

94. *Fonovisa*, 76 F.3d at 262.
95. See MGM Plaintiffs' Opening Brief to the Ninth Circuit in the Kazaa appeal at 58–63.
96. *Ibid.* at 63.
97. s.512(k)(1)(A) defines an OSP for the s.512(a) safe harbour as "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".
98. s.512(k)(1)(B) defines an OSP for the purposes of the other three safe harbours as "a provider of online services or network access, or the operator of facilities therefore, and includes an entity described in subparagraph (A)".
99. *A&M Records Inc v Napster, Inc*, 54 U.S.P.Q.2d 1746 (N.D. Cal. 2000).
1. *Aimster*, 252 F.Supp.2d at 660; *Napster*, 54 U.S.P.Q.2d at 1750.
2. *Aimster*, 252 F.Supp.2d at 661.

article

Viral Online Copyright Infringement in the United States and the United Kingdom: The End of Music or Secondary Copyright Liability? (Part II)[1]

WARREN R. SHIELL

The United Kingdom

Section 16(1) of the Copyright, Designs and Patents Act 1988 ("the CDPA") as amended by the Copyright and Related Rights Regulations 2003 ("the Copyright Regulations") grants to a copyright holder the exclusive right to do any one of the following "restricted acts": copy the work (the reproduction right); issue copies to the public (the distribution right); perform, show or play the work in public (the performance right); communicate the work to the public (the new communication right, which supersedes the old broadcasting and inclusion in a cable programme right); and adapt a work (the adaptation right). Before considering the extent to which copyright holders are protected by the statutory provisions of the CDPA as amended by the Copyright Regulations, we shall first consider the actions that take place between the users of peer-to-peer ("P2P") networks and the providers of P2P software and services that most likely constitute acts of copyright infringement. These include:

(1) the act of "ripping" the audio from a CD and copying it to a computer's hard drive (use A);
(2) copying or uploading an audio file to a folder which is publicly available to other users of a P2P network (use B);
(3) downloading an audio file from a P2P network onto a computer's hard drive (use C);
(4) burning to CD an audio file stored on a computer (use D); and
(5) providing the P2P software and other ancillary services that facilitate uses A, B, C and D (use E).

Traditionally, UK law has drawn a distinction between primary or direct infringement (uses A, B, C, D) and secondary infringement (use E), where a third party does not directly carry out the restricted act but facilitates the direct infringement, although in one recent case[2] the court employed the novel terminology of voluntary and involuntary copying to describe the same distinction. It is submitted that the changes brought about by the Copyright Regulations will not radically affect this distinction between direct and secondary infringement.

Direct infringement

The reproduction right

In the absence of a licence from the copyright holder, uses A, B, C and D clearly violate the reproduction right contained in s.17(2) of the CDPA that states that copying in relation to a literary, dramatic, musical or artistic work is "reproducing the work in any material form. This includes storing the work in any medium by electronic means." Since a copy of an MP3 is invariably stored onto a computer's hard drive, it is probably unnecessary to resort to s.17(6), which extends copying to the making of "transient copies". Under UK law, ever since the Copyright (Computer Software) Amendment Act 1985, references to copying a work in any form has included storage in computer memory. Although the UK government said it considered existing UK law consistent with the Copyright Directive[3] which provides that copying shall be understood in its broadest sense to include "direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part",[4] the Copyright Regulations nevertheless added a new s.182(A)(1) of the CDPA to make explicit the fact that the reproduction right includes copying a recording "which is transient or is incidental to some other use of the original recording".

Dealing with infringing copies

Making MP3s or other audio files publicly available over a P2P network (use B) is arguably a restricted act covered by s.23(d) of the CDPA, which provides that copyright is infringed "by a person, who without the license of the copyright owner distributes

1. The first part of this article appears in [2004] Ent. L.R. 63–71.
2. See *Sony Entertainment (UK) Ltd v Easyinternetcafé Ltd* [2003] W.L. 116984.
3. European Parliament and Council Directive 2001/29 of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, [2001] O.J. L167/10.
4. s.2 of the Copyright Directive.

machine, is an "involuntary copier" and cannot be strictly liable for direct infringement. It was therefore unnecessary for the court to examine the secondary liability issues of the CD burning service.

Providing means for making infringement

Prior to the enactment of the Copyright Regulations, it was questionable whether transmissions in a P2P network would violate s.24(2) of the CDPA. The amended section now provides that copyright in a work is infringed by a person who:

> "without the license of the copyright owner transmits the work by means of a telecommunications system (otherwise than by communication to the public), knowing or having reason to believe that infringing copies of the work will be made by means of the reception of the transmission in the United Kingdom or elsewhere".

Although the importance of this section has been lessened by the public communication right, it may still come into play where files are transmitted otherwise than as a result of being made available "from a place and a time individually chosen" by the recipients, *e.g.* illicit files transmitted in response to specific requests.

The distribution right

Section 18 of the CDPA grants to the copyright holder or licensee the exclusive right to issue copies of the copyrighted work incorporated in a tangible article, including the original, to the public. However, once any particular copy has been lawfully released to the public in the European Union, the distribution right is exhausted. So, for example, a second-hand record shop can sell a used record because that copy (*i.e.* the used record) has previously been put into circulation with the actual or implied consent of the copyright holder. However, the shop infringes the copyright holder's distribution rights if the shop makes duplicate copies of that record which it then sells.[10] Article 3(3) and Recital 29 of the Copyright Directive provide that an authorised communication to the public does not exhaust the copyright holder's further communication to the public rights. Recital 29 explains that the copyright holder's rights are also not exhausted where a user makes a copy of a work from an authorised online service. It is submitted that a typical user of a P2P network issues a copy to the public in violation of the copyright holder's distribution rights when he makes an illicit copy of a song and circulates it on the internet or circulates CD copies burned from unauthorised downloads from a P2P network.

Secondary infringement

Section 24(1)

Some commentators have suggested that P2P providers violate s.24(1) of the CDPA, which provides that copyright in a work is infringed by a person who without license makes, imports, possesses in the course of a business or sells an article "specifically designed or adapted for making copies ... knowing or having reason to believe that it is to be used to make infringing copies". There are two reasons why this provision may not be helpful to copyright holders. First, the House of Lords in *Amstrad* (discussed later in this article) held that where an article is capable of facilitating infringing as well as non-infringing copying (in *Amstrad* it was a twin-deck tape recorder), the supplier must possess more than just generalised knowledge that illicit copying will occur before it will be held liable. Secondly, it is generally understood that the reference to an article "specifically designed or adapted for making copies" is directed at articles such as photographic negatives, moulds and master recordings that are designed to make copies of specific works, rather than at generic copying equipment such as photocopiers or tape recorders. The fact that a proposed amendment to the Copyright Bill that would have changed the wording of the section to "an article designed for making copies of that class of works" was rejected supports this interpretation.[11]

Authorisation

Section 16(2) of the CDPA prohibits any person from "authorising" unlicensed copying or authorising any of the "restricted" acts which are the exclusive acts of the copyright holder, which now include communicating the work to the public (s.20) or making it available to the public (s.182CA) by "electronic transmission in such a way that members of the public may access it from a place and at a time individually chosen by them". In considering whether the provider of P2P software and services might be liable for "authorising" one of the restricted acts, any future court will be bound by the House of Lords decision in *C.B.S. Songs Ltd v Amstrad Consumer Electronics Plc*,[12] in which the court had to consider whether Amstrad had authorised a breach of the 1956 Copyright Act by selling and advertising twin-deck tape recorders which it knew would probably be used for illicit copying although they could also be used for other non-infringing purposes. The case bears many similarities to the US *Sony* decision,[13] particularly in both courts' refusal to impose liability on the seller of an article that facilitated infringement simply because the seller had good reason to know (constructive knowledge) that the article would be used to infringe.

In *Amstrad*, the defendants, BPI, argued that Amstrad's sale and advertising campaign amounted to "authorisation" based on a number of earlier authorities which had treated the term as synonymous with "sanction, approve and countenance".[14] Both the Court of Appeal and the House of Lords rejected this argument on the grounds that "authorisation" requires a "grant or purported grant, which may be express or implied, of the right to do the act complained of". Lord Templeman held that neither the design of the product nor Amstrad's advertising campaign could be construed as authorising unlawful copying, because the ultimate decision to copy was made by the user.[15] As a general rule, a

10. See *Copinger and Skone James on Copyright*, para.7–106.

11. *Hansard*, HL Vol.490, col.1217, and Report of the debates of the House of Commons Standing Committee E in 1988, col.166.
12. [1988] R.P.C. 567.
13. *Sony Corp. of America v Universal Studios, Inc.* 104 S.Ct. 774.
14. *Falcon v Famous Players Film Co* [1926] 2 K.B. 474 at 491 *per* Bankes L.J., following *Monkton v Pathe Freres Pathephone Ltd* [1914] K.B. 395 and *Evans v F. Hulton* [1924] 131 L.T. 534.
15. *Ibid.* at 603.

product that merely facilitated unlawful copying could not confer authority to copy. Also, Amstrad's advertising which drew attention to features which made illegal copying easier nevertheless did not involve a grant or purported grant of authority to copy because copyright warnings made this lack of authority clear to end users.[16] The reasoning of the court was very similar to the *Sony* decision, and both high courts suggested that the outcome could have been different if the defendants in each case had retained control over their products. In *Amstrad*, BPI relied on the second limb of a passage from Laddie, Prescott and Vitoria, *The Modern Law of Copyright* (1980), cited by the Australian High Court in *R.C.A. Corp v John Fairfax & Sons Ltd*, that:

> "a person may be said to authorise another to commit a tort of infringement if the one has some form of control over the other at the time of infringement or, if he has no control, is responsible for placing in the other's hands materials which by their nature are inevitably to be used for the purpose of infringement".[17]

Lord Templeman only said that this proposition was stated too widely. Slade L.J. in the Court of Appeal only rejected the second limb of this proposition. Lord Templeman also cited with apparent approval dicta from another Australian case, *Moorhouse v University of New South Wales*,[18] in which Gibbs J. stated 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".

In that case, the Australian High Court held a university liable for supplying photocopying machines in their library and not taking reasonable steps to prevent unlawful copying. Lord Templeman's commenting on *Moorhouse* that "Whatever may be said about this proposition, Amstrad have no control over the use of their models once they are sold" leaves the door open for holding a person liable for authorising where they have some control over the means of infringement. Lord Templeman also referred to a case of first impression, *C.B.S. v Ames Records & Tapes Ltd*,[19] where the court refused to hold a record store retailer liable for renting out records and selling blank tapes. Even though the retailer had good reason to know that the records would probably end up being copied, the court held that he did not authorise copying where the records contained MPCS copyright warnings and customers completed sign-out forms containing similar warnings. However, Whitford J. suggested that the *Moorhouse* principles would have applied had the retailer installed copying equipment in his shop and had thus retained control over the means of infringement.[20] Whitford J. referred to the Privy Council's decision in *Vigneux v Canadian Performing Right Society Ltd*,[21] cited with approval by both Lawton and Glidewell L.JJ. in *Amstrad*, which refused to hold the supplier of coin-operated jukeboxes liable for authorising copyright infringement on the grounds that once the equipment was hired out, the supplier no longer had any control over its use. Glidewell L.J. concluded: "In my view, a person cannot 'authorise' an act unless he has the power to either permit the act or to prevent it. Once Amstrad have sold the equipment to a retailer, they have no control over its use by the eventual purchaser."

In applying *Amstrad* to any future P2P provider, the courts will face many of the same issues now facing the American courts in determining liability for contributory and vicarious liability. First, a court will have to consider whether the control requirement means that a P2P provider has the present technical ability to stop or prevent infringement on its network, as in the *Grokster* case, or some lesser degree of control such as keeping out particular users who are identified as known infringers. What if a court finds that a P2P provider has deliberately configured its software or network to avoid such control (and therefore legal liability) but concludes that the system could be easily modified to prevent infringement at minimal cost?

Secondly, what kind of knowledge should be sufficient to fix liability? Sections 97A and 191JA of the CDPA as amended by the Copyright Regulations require that "a service provider has actual knowledge of another person using their service to infringe copyright" before an injunction can be issued by the High Court. Both sections contain provisions that:

> "(2) In determining whether a service provider has actual knowledge for the purposes of this section, a court shall take into account all matters which appear to it in the particular circumstances to be relevant, and amongst other things, shall have regard to—
>
> (a) whether a service provider has received notice through a means of a contact made available in accordance with regulation 6(1)(c) of the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013); and
>
> (b) the extent to which such notice includes—
>
> (i) the full name and sender of the notice;
>
> (ii) details of the infringement in question."

A P2P provider would normally meet the definition of "service provider" as a provider of "Information Society Services"—that is "any service normally provided for remuneration, 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 the service".[22] Also, Recital 18 to the E-Commerce Directive provides that providing access to a communications network can be an Information Society Service.

16. *ibid.* at 604.
17. [1982] R.P.C. 91.
18. [1976] R.P.C. 151.
19. [1982] Ch. 91.
20. *ibid.* at 118. The hypothetical posed by Whitford J. would have looked remarkably like the circumstances of the *Easyinternetcafé* case, and it is unfortunate that the court in that case declined to analyse the defendant's "CD burning service" in such terms.
21. [1945] A.C. 108.
22. This is a summary definition contained in the Directive 2000/31 of the European Parliament and of the Council of June 8, 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), [2000] O.J. L178/1 ("the E-Commerce Directive"). For a complete definition of "service provider", the Copyright Regulations refer to reg.2 of the Electronic Commerce (EC Directive) Regulations 2002, which refers to the definition in Art.2(a) of the E-Commerce Directive, which itself refers to definitions in Art.1(2) of the Technical Standards Directive 98/34 as amended by Directive 98/48.

It is significant that this definition of "service provider" is much broader than the commonly understood meaning of "internet service provider" and does not require an information service provider to maintain an ongoing relationship with its users or exercise ongoing control over the network. However, the Copyright Regulations contain little guidance on the meaning of actual knowledge, particularly the time frame during which it must be acquired and to what extent it must relate to actual knowledge of specific cases of infringement by specific users. The American case law should provide a lesson in how difficult it can be to resolve this question. Those cases suggest that it is easier to attribute actual knowledge of infringement to centralised P2P providers, such as Napster, which operate and control an integrated network, by the sending out of notices of infringement than decentralised providers, such as Kazaa or Grokster, which claim that they merely supply software platforms and have no control over how their software is used. In such cases where notices of infringement have been sent out after software has been downloaded by individual users, P2P providers, at least in the United States, have been successful in arguing that they cannot be imputed with actual knowledge when the notices arrive at a time when it is too late for them to be acted upon.[23] The logic of the argument is clearer when applied to the sale of a product. For example, applying it to the facts of *Amstrad*, it would be like arguing that Amstrad would have had actual knowledge of infringement if it had received notices that certain buyers were using its tape recorders to illicitly copy after the products had been sold. Earlier in this article, it was suggested that the issue in the American courts has been unduly complicated by a failure to distinguish between the supply of an article of software or software platform and the operation of a network/ service, and hopefully the UK courts will not get bogged down in the same confusion.

Joint tortfeasors

Could a P2P provider be liable for copyright infringement as a joint tortfeasor along with direct infringers? In *Amstrad*, the court rejected BPI's arguments that Amstrad was liable as a joint tortfeasor by drawing upon a number of old patent decisions which decided that a person could not be liable for patent infringement for selling materials even if he knew they would be used for infringement.[24] Lord Templeman stated the general rule that: "joint infringers are two or more persons who act in concert with one another pursuant to a common design".[25] The court decided that there was no common design to infringe between Amstrad and customers because the tape recorders were capable of being used for lawful and unlawful purposes and "manufacturers and retailers are not joint infringers if purchasers choose to break the law". In *Unilever Plc v Gillette (UK) Ltd*,[26] a case concerning the liability of a parent company for an alleged patent infringement committed by its subsidiary, Mustill L.J., analysing the history of joint tortfeasance, stated that "the proposition that participation in a common venture may cause someone to become directly liable as tortfeasor, together with someone who actually did the damage"[27] was settled law. In particular, he drew attention to a 1928 case, *Brook v Bool*,[28] where a landlord was held liable as a joint tortfeasor for an explosion negligently caused by a lodger he had retained to investigate a gas leak in his shop. Judge Salter in that case applied the *Koursk* decision (cited by Lord Templeman in *Amstrad*) in finding that the landlord and the lodger were both responsible because they were engaged in a joint enterprise. The court was clear that this form of enterprise liability was quite distinct from the other ground on which the defendant was held liable—namely the control he had over the proceedings.[29] Mustill L.J. then explained what it means to act in concert pursuant to a common design:

> "The idea does not, as it seems to me, call for any finding that the secondary party has explicitly mapped out a plan with the primary offender. Their tacit agreement will be sufficient. Nor, as it seems to me, is there any need for a common design to infringe. It is enough that the parties combine to secure the doing of acts which in the event prove to be infringements."[30]

It will be interesting to see how far a court will be willing to go in deciding that a P2P provider's knowing and continuing provision of software and services to maintain a predominantly infringing network constitutes acting in concert pursuant to a common design. It is suggested that the following factors might be helpful in answering that question:

- Does a provider sell an article or does it maintain an ongoing relationship with the users of its products or services which are used to infringe?
- Does a provider continue to operate and maintain an environment or site knowing or with good reason to know that widespread infringing activity is taking place there?
- Is the article or site used primarily for infringing purposes?
- What reasonable steps could be taken to minimise infringing activity when a provider becomes aware or should be aware that an article or site is being used for infringing activity?
- What are the economic costs to both the provider and the copyright holder of modifying their works or products/ services to minimise infringement? For example, could this be accomplished by a software modification by the P2P provider or the incorporation of anti-copying technology into copyrighted works at minimal cost?

23. See *MGM Studios, Inc v Grokster*, 259 F.Supp.2d at 1037.
24. *Townsend v Haworth* (1875) 48 L.J. Ch. 770n, followed in *Dunlop Pneumatic Tyre Co Ltd v David Mosely & Sons Ltd* [1904] 1 Ch. 164, cited in *Belegging-en Exploitatiemaatschappij Lavender BV v Witten Industrial Diamonds Ltd* [1979] F.S.R. 59. It is worth noting that at about the same time as this was decided, an American court was reaching the opposite result where a merchant was held liable for selling printing plates he knew would be used to infringe copyright: see *Harper v Shoppel*, 28 F. 613 (SDNY 1886).
25. *Amstrad* [1988] R.P.C. at 606, citing Scrutton L.J. in *The Koursk* [1924] P. 140.
26. [1989] R.P.C. 583 at 603.
27. *Ibid.*
28. [1928] 2 K.B. 578.
29. *Ibid.* at 584. This form of vicarious liability, similar to the American case law, has not been further developed, although the case was briefed but not cited in the *Amstrad* appeal.
30. *Ibid.* at 608, cited with approval in *MCA Records Inc v Charly Records Ltd* concerning the joint liability of a director for his company's infringement by copying and issuing unlicensed copies Chess Recordings in the United K.

- Does the provider have the right and ability to supervise the use of its products or the site where infringing activity is taking place?
- Is an article or service specifically designed or adapted to facilitate infringement?
- Has the provider incited or procured copyright infringement by specific users?
- Does the provider receive a direct or indirect commercial benefit from the infringing activity?

Defences to infringement

The home copying exception

Unlike the United States, the United Kingdom has no concept of "fair use", although c.III of Pt I of the CDPA contains a number of "fair dealing" exceptions: for example, permitting certain acts to be carried out for the purposes of non-commercial research or for the purpose of criticism or review. The Copyright Regulations do not alter this basic approach but they do carve out important new protections designed to protect home copying and temporary copying by intermediaries which is part of a technological process. However, it is unlikely that users of illicit P2P networks or P2P providers will benefit from the new protections.

Article 5(2)(b) of the Directive gave Member States the option of including a "home copying exception" in their legislative schemes for "natural person[s] for private use and for ends that are neither directly nor indirectly commercial". The UK Government declined to give full effect to such a broad "home copying exemption", instead amending the existing "time shifting" provision contained in s.70 and para.17 of Sch.2 to the CDPA that exempts copying of a recording of a broadcast provided it is made in a domestic premises, is for private and domestic use, and is made solely for the purpose of enabling it to be viewed or listened to at a more convenient time. Thus, in the absence of any express or implied contractual license, burning copies of CDs from other CDs or copying CDs to a computer (use A) are still technically restricted acts. Furthermore, since internet transmissions are generally excluded from the definition of "broadcast" unless they are part of a scheduled programme, concurrent transmis-sions of a live event or simultaneously transmitted by some other means, downloading files from a P2P network (use C) is not protected.[31]

Temporary copies made as part of technological process

A new s.28A and para.1A of Sch.2 to the CDPA gives effect to Art.5.1 of the Directive designed primarily to protect ISPs' caching and browsing functions. Article 5.1 provides that:

> "Temporary acts of reproduction referred to in Article 2, which are transient or incidental, and an integral and essential part of a technological process and whose sole purpose is to enable:
>
> (a) a transmission in a network between third parties by an intermediary or
>
> (b) a lawful use
>
> of a work or other subject matter to be made, and which have no independent significance, shall be exempted from the protection right provided for in Article 2."

Recital 33 of the Copyright Directive explains that the protection is designed to cover temporary acts of caching and browsing where an intermediary does not modify or extract data from the temporary copies for unlawful uses, and that a use is considered lawful where it is authorised by the right holder and not restricted by law.

Section 28A of the CDPA implementing the Directive states that copyright is not infringed

> "by the making of a temporary copy which is transient or incidental, which is an integral and essential part of a technological process and the sole purpose of which is to enable—(a) a transmission of the work in a network between third parties by an intermediary; or (b) a lawful use of the work; and which has no independent economic significance.

The main reason why P2P providers and end users are unlikely to benefit from these new protections is that the Directive makes it clear that they are designed to protect acts of temporary copying that would otherwise be a violation of the reproduction right and not other restricted acts that might incidentally involve a temporary act of copying. In other words, where primary or secondary liability accrues as a result of a violation of some other restricted act (*e.g.* the communication to the public right or distribution right), the new protections should not apply simply because in the process of violating that right a temporary act of copying took place that would fall otherwise within the definition.

In addition, as a factual matter, none of the uses A–D typically undertaken by end users come close to meeting the definition of making a temporary copy for either a lawful use or transmission in a network between third parties by an intermediary. Consider the use B scenario which violates the communication to the public right. An end user typically downloads P2P software containing instructions that all file downloads from the network are copied to shared directories that are available to everyone else connected to the network unless the user deletes individual files he does not want to share or changes the default settings so that downloads are not automatically stored in a shared directory. The user also has the option of adding other files to the shared directory. When the user intentionally and voluntarily saves illicit copies to a publicly accessible directory, either by copying individual files or by configuring his P2P software to do this automatically from files he has downloaded (a direct use C), he neither makes temporary or transient copies, nor does he act as an intermediary making transient copies as part of a technological process to enable either a lawful use of the work or transmission between third parties. Lastly, his actions have an "independent economic significance" to the copyright holders since they undermine the market for the work. The only conceivable situation where an end user might be able to claim the benefit of the section is where a P2P software platform contains a hidden proxy caching system of which users are unaware. It is then conceivable that such a user might download software and use the network for legitimate purposes unaware that their system is caching infringing materials.[32] However, copyright holders can still argue that such proxy caching has "independent economic significance".

31. s.6(1A) of the CDPA.

32. Niklas Zennstrom, who co-founded Kazaa, has developed a caching system for use with his FastTrack P2P protocol network. See "P2P Caching: Unsafe at Any Speed?", available online at *http://news.com.com/2102-1025-3-1027508.html*.

Also, P2P providers are unlikely to benefit from the protection of the provisions since most P2P networks are structured to leave the copying and storage functions to individual end users' computers. Even if P2P providers add proxy caching facilities to their networks, the protections may still not apply because liability is unlikely to arise as a result of a violation of the reproduction right, and proxy caching by such a network is likely to have an "independent economic significance" if it enables widespread copyright infringement.

Finally, Recital 59 of the Copyright Directive suggests that copyright holders should have the right to seek injunctive relief against an intermediary who carries infringing network even if the acts carried out by the intermediary are exempted under Art.5. It states that the conditions and modalities of such works should be left to the national law of Member States. The Copyright Regulations are silent on the issue.

The Electronic Commerce (EC Directive) Regulations 2002

There is a certain amount of overlap between the temporary copying protections contained in the Copyright Regulations and the E-Commerce Regulations (the UK equivalent of the DMCA "safe harbours") that implement the E-Commerce Directive of 2000.[33] Like the DMCA, the Regulations are designed to protect intermediaries that play a passive, largely technical role in transmitting and storing data from third parties. The Regulations contain "mere conduit", "caching" and "hosting" exemptions like the United States' Digital Millennium Copyright Act ("DMCA"), but no equivalent of the DMCA, s.512(d) "Information Tools Locator". Another major difference is that the European safe harbours only offer protection against monetary awards and criminal penalties, whereas the DMCA also limits the scope of injunctive relief.[34]

The "mere conduit" exemption protects a "transmission in a communication network of information provided by a recipient of the service or the provision of access to a communication network". The service provider must not initiate the transmission, select the recipient, or select or modify the information contained in the information.[35] Notwithstanding that "communication network" is nowhere defined in the Regulations or the Directive, the exemption goes much further than its DMCA counterpart, since all that is required is the "provision of access to a communications network" without any finding that the network be controlled or operated by the service provider.

However, there are several reasons why a P2P provider would probably fall foul of the exemption. First, common sense and the intent of the E-Commerce Directive dictates that the phrase "shall not be liable ... as a result of that transmission" should be read narrowly to ensure that protection is only offered where exposure to liability arises solely by virtue of the passive technical process identified in the mere conduit safe harbour. The caching and hosting exemptions have similar wording and the same interpretation should apply. Accordingly, the exemptions should not protect providers whose liability arises by virtue of some other cause of action (e.g. authorisation, joint tortfeasance) simply because information is then automatically transmitted, cached or hosted on their systems. Secondly, all the exemptions need to be read in conjunction with Recitals 42–44 of the E-Commerce Directive, which state that the exemptions are not designed to protect service providers that have knowledge or control over information which is stored or transmitted, or that "deliberately collaborate with one of the recipients of the service in order to undertake illegal acts".

The "caching" and "hosting" exemptions contain additional conditions making it unlikely that a P2P provider could seek protection from their provisions. Regulation 18 (caching) does not protect service providers who do not act expeditiously to remove or disable information "upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or administrative authority has ordered such removal or disablement". Regulation 19 (hosting) does not protect service providers who know or have reason to know of unlawful activity, or if they have such knowledge or awareness do not act expeditiously to remove or disable access to such information.

Conclusion

Ignoring the political and wider social issues that attend the debate about the role of copyright in stemming internet piracy, the American case law discussed in the first part of this article provides an instructive framework for UK policy-makers analysing secondary liability; however, it should also serve as a warning about the dangers of creating overly rigid classifications. In particular, any future UK court should be clear on whether it is applying a "control"-based theory which grounds liability in a provider's ability to control infringing activity, which more closely corresponds to the cases on authorisation, or "an enterprise"-based theory rooted in the concept of joint tortfeasance which penalises voluntary participation in tortious activity.[36]

33. Directive 2000/31/EC of the European Parliament and of the Council of June 8, 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), [2000] O.J. L178/1.

34. Arts 12, 13 and 14 of the E-Commerce Directive state: "This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent infringement."

35. Reg.17 implementing Art.12 of the E-Commerce Directive.

36. The Lieber plaintiffs make a similar point in their opening brief to the Ninth Circuit in the *Grokster* appeal at 23–24.