Copyright in the Age of Distributed Applications

Seth D. Greenstein
Partner, McDermott, Will & Emery
Counsel, Digital Media Association
Washington, D.C.
sgreenstein@mwe.com

Abstract

This paper explores the pressures exerted on traditional principles of copyright liability and enforcement when networking software applications that are specifically designed to exchange copyrighted works -- thus inherently having both infringing and non-infringing uses -- become widely disseminated and virally popularized.

Existing copyright case law imposes liability on third parties for the infringing acts of others, based on the third party's ability to exercise effective supervision over those acts or knowledge that certain devices or facilities could not be used for substantial purposes other than for infringement. New technology, and the complex and uncertain task of discerning what constitutes a noninfringing or fair use of such technology, challenges these principles from the perspectives of both copyright owners and the public interest. One response has been to enact non-copyright legislation to address, through imperfect balances, the economic consequences of unauthorized access to and copying of copyrighted works. The 1992 Audio Home Recording Act ("AHRA") immunizes certain audio recording devices and personal uses against the threat of infringement claims, in return for mandated royalty payments and technological protection measures to remedy alleged economic harm to copyright owners. The 1998 Digital Millennium Copyright Act ("DMCA") proscribes certain services and technologies used to circumvent technological protections, without regard to whether circumvention leads to infringement or fair uses.

Recently, technologies have been developed that obsolete traditional concepts underlying the standards for imposing third party liability for infringement. Software applications such as Napster create a virtual telecommunications network by which a community of thousands of simultaneous users exchange copyrighted works (in both

infringing and noninfringing acts), without the ability to monitor or control, in advance, user conduct. Software such as Gnutella applies a different topology in which there is no centralized server or control agent, such that each user becomes a server along the network. For such distributed network technologies, infringing activity becomes efficient and widespread; legal enforcement against each individual infringer is impractical, if not impossible; and there is no central authority (other than the creator of the software) to seek to hold liable for infringing user activity.

The paper explores how traditional legal analysis might adapt to these technologies while maintaining the traditional balance between the rights of copyright owners and the privileges of copyright users, and giving due regard for the intellectual property rights of technology companies and the progress of technology. Specifically, the paper suggests additional factors that should inform any decision on third party liability, including the evaluation of:

- The nature of each potential noninfringing use;
- The likelihood that any consumer would acquire and use the product for these noninfringing purposes;
- The role of the technology in facilitating the infringing uses;
- The role of the technology in facilitating the noninfringing uses;
- The likelihood that, if the technology is or is not deemed to be infringing, that noninfringing uses will proliferate; and,
- The impact that a finding of infringement would have upon the technology and technological progress.

Distributed Network or "Peer-to-Peer" Applications

The Internet generally operates as a system of service providers providing access for subscriber clients that access data from host servers. This model created its own set of legal issues for companies that provided the backbone of the telecommunications infrastructure, such as AT&T, Sprint and MCI; Internet service providers, such as Netcom, UUNet and Concentric Networks; online service providers, such as America Online and Compuserve; "post your own" personal website hosts such as Geocities; and information location tools, such as Yahoo!. District court decisions suggested that in certain factual circumstances such providers could, as a matter of law, be held liable for the infringing acts of their subscribers.[1] In response, Congress enacted a "safe harbor" immunity for these providers against claims of vicarious liability and contributory infringement arising from the actions of their subscribers and customers.[2]

Even after passage of the DMCA, copyright owners threatened legal action against search engines tailored to the location of copyrighted material, including search engines which facilitated searching for music files encoded in the MP3 format.[3] Settlements between copyright owners and the sites reportedly followed the DMCA Title II model whereby the site promised to disable links to files identified by the copyright owner as unauthorized and infringing.[4] The recording industry also pursued schools and

---

1 See Religious Tech. Center v. Netcom On-Line Communication Serv., Inc., 907 F. Supp. 1361 (N.D. Cal. 1995).

2 Title II of the DMCA, 17 U.S.C. § 512.

3 MP3 is a voluntary audio file format standard adopted by the Motion Picture Experts Group in the late 1980's as the audio layer 3 of the MPEG-1 audiovisual format. Based on technology from the Fraunhofer Institute, MP3 has become the Internet music format of choice because it reproduces quality sound in a file compressed more than 10 times smaller than the CD Red Book audio format. Unlike other formats such as CD audio or DAT, MP3 lacks any "flag" bits that indicate whether the file may be copied, or other technological protections that might inhibit copying and distribution.

4 See http://www.riaa.com/News_Story.cfm?id=69.

individuals who hosted large numbers of music files, prosecuting one student under the so-called "No Electronic Theft" Act of 1997.[5]

In mid-1999, a new technology now known as "peer-to-peer" file sharing emerged under the name "Napster." This software altered the typical "end-to-end" Internet topology by permitting searching, identification and direct exchange between individual users of music files in the MP3 format. This topology is shown generically in Figure 1:

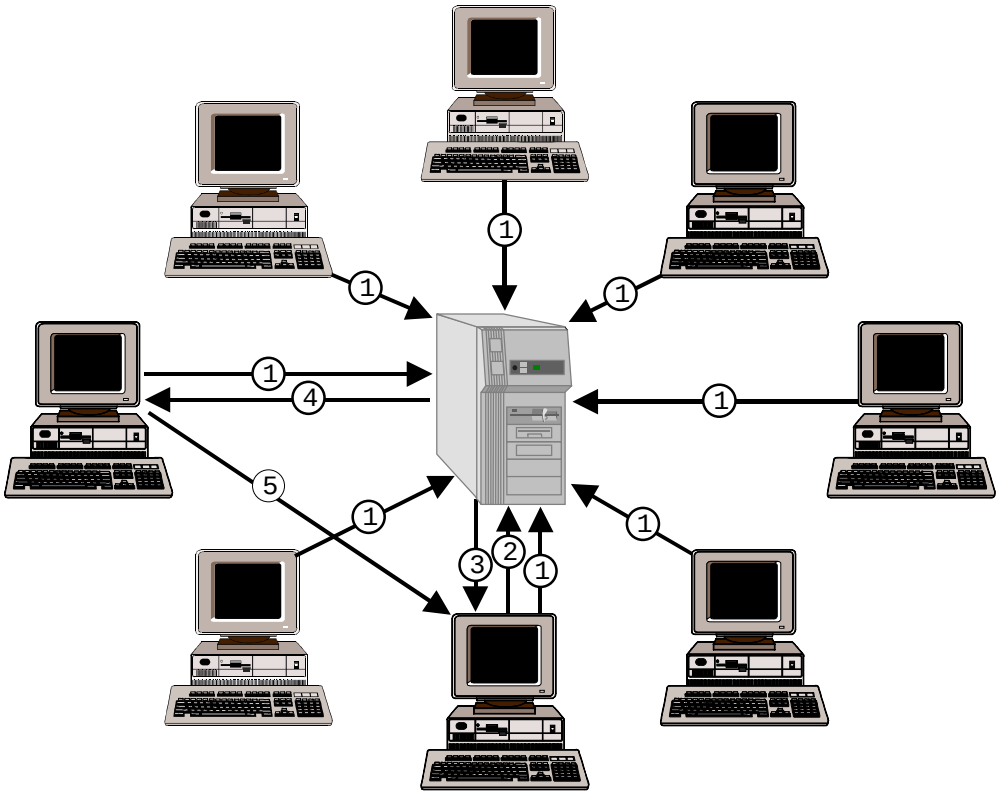

Figure 1: Topology of a Centralized Server in a Distributed Networking Application

The Napster software essentially provides a client browser interface to a host server search engine for the network of users of its software, that enables the users to search for and share music files with other Napster users online at that particular time. In Figure 1, the server in the middle represents the server owned by Napster, Inc.; around the perimeter are PCs currently running the Napster client browser. When a user starts the Napster program, the program communicates to a Napster server the names of all

[5] Public Law 105-147, 111 Stat. 2678. See http://news.cnet.com/news/0-1005-200-346316.html

MP3 files that the user offers to share with other users. (This communication is illustrated above in the lines numbered (1).) These file names (which are created by the user) are entered into Napster's database of files then available online from persons then using the Napster software. The database changes dynamically each time a user starts or exits the Napster program.

Using the Napster browser, a Napster user can place a search request by artist name or song title, shown above as line (2). The Napster server searches its central database of file names, and returns a list of files from any Napster users then online who have on their hard disk drives files responsive to the search request, illustrated as line (3). The Napster software displays the search request results with the names and attributes of those files, including file size, bit rate and transmission speed. If the user selects a file for downloading, the Napster server instigates transmission of the file via file transfer protocol from the other user's computer, as shown in line (4), to the requesting user's computer, as shown in line (5). Napster's servers neither store any music files nor copy any of the music files being transferred between computers.

Essentially, the Napster server acts as a traffic cop allowing communication among Napster users and, with respect to the search and download functionality, makes the users' computers the equivalent of individual servers that the Napster server networks together. The Napster software verifies that the files are using the MP3 data file format. However, nothing inherent in the MP3 data allows Napster to determine whether the file contains music or other sound, whether the data constitutes copyrighted material, whether such material has been authorized for transmission or file-sharing, or whether the music contained in that file is, in fact, the song identified in the name of the file.

Without any advertising (other than the flood of press articles generated by copyright controversies),[6] and without generating any revenue, Napster reportedly has

---

[6] On December 6, 1999, 18 recording companies filed suit against Napster based on contributory infringement and vicarious liability. On July 26, 2000, Judge Marilyn Hall Patel entered a preliminary injunction against Napster, finding that plaintiffs had established a likelihood of success on the merits of both claims. The injunction was stayed two days later by the Ninth Circuit Court of Appeals. On August 11, 2000, Judge Patel issued her written opinion addressing the preliminary injunction motion, http://www.cand.uscourts.gov/cand/tentrule.nsf/4f9d4c4a03b0cf70882567980073b2e4/74

attracted more than 20 million users worldwide. Other technologies, such as Macster (for Apple users), ScourExchange and CuteMX follow this same topographical model.

In March 2000, two America Online programmers who had previously created the popular Winamp program for playing MP3 files released a more decentralized file-sharing technology. The program, known as Gnutella, was notable in at least three key respects. First, Gnutella enabled searching and sharing of all file types, including music, motion pictures, images and text. Second, Gnutella was an "open source" program, meaning that the program code was published for copying, implementation and enhancement, without any assertion of either copyright or commercial rights. Third, and most relevant to this analysis, Gnutella does not require a central server to connect users. The topology of this decentralized distributed network application is shown as Figure 2:

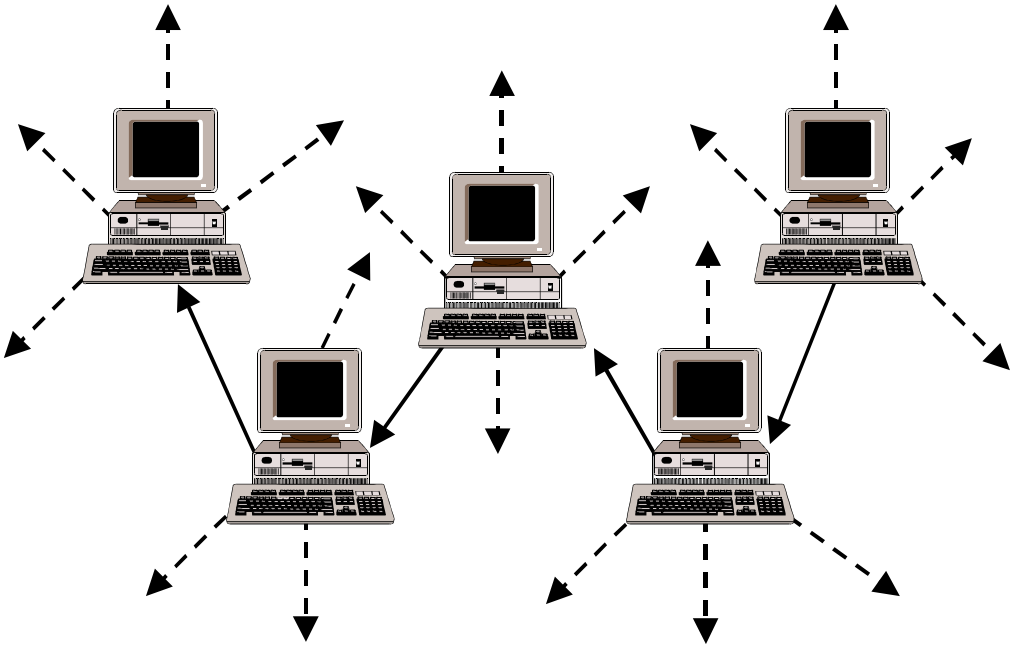

Figure 2: Decentralized Distributed Application Network Topology

Each Gnutella user must know the Internet Protocol address of at least one other Gnutella user then online. Once connected, each Gnutella user becomes a server connected to any and every computer along the network, as shown by the dotted-lined arrows in Figure 2.

---

bf2867dde99f0f88256938007a1205/$FILE/NapsterF%26C2.pdf (hereinafter referred to as "Napster II").

Every search request by a Gnutella user can generate results directly from all other online Gnutella users, in a search path shown on Figure 2 by the solid-lined arrows.[7]

Most recently, a programmer in the United Kingdom created a peer-to-peer networking program known as "Freenet," which operates along the same general topological model as Gnutella. Freenet reportedly is designed with a more efficient method of searching for material by mirroring popular content across the network to speed transactions. Freenet protects user and publisher anonymity so that not even the host computer may know what data it stores for access via the Freenet network. As such, Freenet's author has articulated its mission as less to locate media files than to promote democratic values, thwart efforts to censor the Internet and secure the free exchange of ideas against potential intervention by governmental and other policing authorities.[8]

Rights Implicated by Distributed Network Applications

Under the Copyright Act, copyright owners are granted five discrete exclusive rights, including (as most relevant to this paper) the rights to reproduce the work in copies and to distribute copies of the work.[9] Certain copyrighted works may consist of

---

[7] See http://www.gnutella.wego.com/.

[8] See http://freenet.sourceforge.net/.

[9] Section 106 provides:

> Subject to sections 107 through 120, the owner of copyright under this title has the exclusive rights to do and to authorize any of the following:
>
> (1) to reproduce the copyrighted work in copies or phonorecords;
>
> (2) to prepare derivative works based upon the copyrighted work;
>
> (3) to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending;
>
> (4) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works, to perform the copyrighted work publicly;
>
> (5) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work, to display the copyrighted work publicly; and
>
> (6) in the case of sound recordings, to perform the copyrighted work publicly by means of a digital audio transmission.

more than one copyrightable work. Copyrights in a downloaded music file can subsist separately in both the underlying musical works (the composition as written) and the sound recordings (the performance of that composition). Motion pictures are copyrightable in the whole, but may also include copyrightable material in the screenplay (and the book or story on which it may be based) and musical works included in the soundtrack. The five rights to each of these works may be held by distinct copyright owners and administered separately by different entities or collecting societies.

The exercise of any of these rights, unless authorized by the copyright owner or by an exemption or defense established by statute or case precedent, constitutes copyright infringement.[10] Direct copyright infringement occurs when the defendant itself exercises any of the rights without authorization of the copyright owner or the law. The defendant's intent/knowledge is *not* an element of direct infringement, inasmuch as even innocent infringers deprive copyright owners of their rights and infringers could easily claim a lack of knowledge of the infringement as a defense.[11]

The use of distributed network applications could implicate the following rights (without consideration of whether the particular use constitutes infringement):

Distribution Right

- By launching the program, the user authorizes the distribution of files containing copyrighted works.
- By permitting downloading, the user distributes a copy of files containing copyrighted works.

Reproduction Right

- Copying the works to a computer hard drive in order to make such files available for distribution.
- Recording downloaded files to a hard drive or other storage medium.

---

[10] Sony Corp. of America v. Universal City Studios, 464 U.S. at 417, 432-33, 104 S. Ct. 774, 784, 78 L. Ed.2d 574 (1984).

[11] See Playboy Enter., Inc. v. Frena, 839 F. Supp. 1552, 1559 (M.D. Fla. 1993).

Traditional Standards for Imposing Third Party Liability

Historically, copyright owners have refrained from suing individuals for personal, noncommercial infringing conduct. Copyright owners from time-to-time have pursued particularly egregious offenders, hoping to establish valuable legal precedents and instill *in terrorem* respect for copyright. Users of distributed network applications could be subject to liability to copyright owners for any direct infringements. However, these systems can obscure or protect individual user identities, and the magnitude of users makes litigation for direct infringement an impracticable if not impossible method of enforcement. Moreover, individual infringers are generally unable to adequately compensate copyright owners through statutory or actual damages, or to reimburse litigation costs through awards of attorney fees.

The more logical approach has been to hold responsible a third party in situations where, by having a "deeper pocket," there is a greater potential reward for the litigation efforts; or where, by virtue of being higher up in the chain of infringement, the imposition of liability will deter or enjoin a substantial number of infringing acts. Third party liability traditionally has been imposed under one of two legal theories, vicarious liability or contributory infringement, as described below.

Vicarious Liability

Vicarious liability focuses on the relationship of the third party with the direct infringer.[12] Courts impose vicarious liability for the actions of the direct infringer where the defendant has both (1) the right and ability to control the infringer's actions, and (2) received a direct financial benefit from the infringement.[13] Liability may be found even though the defendant neither knows of nor encourages the infringing activity.[14]

The early cases addressing indirect liability under the copyright law arose primarily in two contexts. In the "landlord-tenant cases,"[15] a landlord leases property to a

---

[12] Religious Tech. Center v. Netcom On-Line Communication Serv., Inc., 907 F. Supp. at 1375.

[13] Fonovisa Inc. v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996).

[14] Shapiro Bernstein & Co., v. H.L. Green Co., 316 F.2d 304, 307 (2d Cir. 1963).

tenant who engages in copyright infringement on the leased premises,. In such cases, the courts generally found the degree of control and the relationship between rental payments and the infringement too tenuous to impose liability. However, in the so-called "dance hall cases,"[16] a dance hall owner or manager hires a performer who performs copyrighted material without the permission of the copyright holder. Generally, courts find the degree of control and the relationship between the remuneration and infringement sufficient to impose liability. Some examples of cases finding vicarious liability:

- In Shapiro Bernstein & Co. v. H.L. Green Co., Green, the owner of a chain of department stores, licensed Jalen to run its record department in twenty-three stores. Plaintiffs, copyright holders of popular musical compositions, alleged that Jalen directly infringed their copyrights by manufacturing bootleg recordings containing copyrighted works without obtaining a license. The court held Green vicariously liable for selling the bootlegged recordings because it had both the power to exercise control over the infringing activity and a "direct financial interest in the exploitation of copyrighted materials – even in the absence of actual knowledge that the copyright monopoly is being impaired."[17]
- In RCA/Ariola International Inc. v. Thomas & Grayston Co.,[18] owners of retail stores that allowed customers to use for a fee audio cassette duplicating machines were held liable for direct infringement where their employees actively participated in the infringing duplication of copyrighted prerecorded cassettes. Metacom, the manufacturer of the cassette duplicating machines, and the

---

15 Deutsch v. Arnold, 98 F.2d 686 (2d Cir. 1938); Fromont v. Aeolian Co., 254 F. 592 (S.D.N.Y. 1918).

16 Buck v. Jewell-LaSalle Realty Co., 283 U.S. 191, 198-99 (1931); Dreamland Ball Room, Inc. v. Shapiro, Bernstein & Co., 36 F.2d 354 (7th Cir. 1929); M. Witmark & Sons v. Tremont Soc. & Athletic Club, 188 F. Supp. 787 (D. Mass. 1960); Renmick Music Corp. v. Interstate Hotel Co., 58 F. Supp. 523 (D. Neb. 1944), *aff'd*, 157 F.2d 744 (8th Cir. 1946).

17 316 F.2d at 308.

18 845 F.2d 773 (8th Cir. 1988).

manufacturer's president, were found liable as vicarious infringers because they retained ownership and control over the machines.

- In Fonovisa Inc. v. Cherry Auction, the court allowed the plaintiff to proceed against the owner of a swap meet for renting space to record bootleggers, where the defendant had the right and ability to control the activities of vendors, and derived a financial benefit from admission and parking fees and concessions.[19]

b. Contributory Infringement

Contributory infringement occurs when one person knowingly induces another to directly infringe the copyright or materially contributes the direct infringing activities of another.[20] In Gershwin, for example, ASCAP brought an infringement action against an organization ("CAMI") that managed concert artists and promoted their concerts. The court held CAMI liable as a contributory infringer on the basis that CAMI knew that its artists included copyrighted compositions in their performances without securing licenses from the copyright holders; and in providing the audience and promoting the concert, CAMI had the requisite level of participation to be found liable. In the Netcom case, the court held that although the service providers were not direct infringers, they could be liable for contributory infringement. The court found that notice from the copyright owner was sufficient to raise a question of fact as to whether Netcom and the BBS owner knew or should have known of the infringement; and that providing services that distributed the infringing material constituted substantial participation in the infringing activity.[21] However, the court stated that a mere unsupported allegation of infringement by a copyright owner may not automatically provide an ISP with notice of an infringing activity, and so the court did not impose on either Netcom or the BBS operator an obligation to independently investigate infringement absent notice.[22]

---

19 76 F.3d 259 (9th Cir. 1996).

20 See Gershwin Publ'g Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (2d Cir. 1971).

21 Netcom, 907 F. Supp at 1374-75, 1382.

22 Id., 907 F. Supp. at 1374.

Contributory infringement liability also may be found where the defendant provides the instrumentality used to commit a direct infringement by another. For example, a court issued a preliminary injunction against a BBS operator who sold copiers used to reproduce copyrighted video games.[23] Similarly, contributory liability was imposed upon a seller of cable descrambling chips used in the infringing activity of consumers.[24] In each of these two cases, however, the particular devices at issue were not capable of substantial noninfringing uses. Because the devices lacked such noninfringing uses, the court reasonably could find that the manufacturer had knowledge of the infringement sufficient to impose liability as a contributory infringer.

The "Sony" Standard

In 1984, the Supreme Court enunciated a standard for analyzing when the manufacturer of a device might be held liable for contributory infringement. Where the device at issue is a "staple article of commerce" that can be used for multiple purposes, the Court held that it is not enough that a manufacturer knows that the equipment might be used for infringing purposes. The defendant will be deemed a contributory infringer only if the items are not capable of "substantial" or "commercially significant" noninfringing uses.[25] In addressing the contributory liability of the Sony Betamax Video Cassette Recorder, the Court held that the sale of copying equipment does not constitute contributory infringement if that product is "widely used for legitimate, unobjectionable purposes"; and that, "indeed, it need merely be capable of substantial noninfringing uses."[26] Applying this standard, the Court found that the manufacturer of a videocassette

---

[23] Sega Enters. Ltd. v. MAPHIA, 857 F. Supp. 679 (N.D. Cal. 1994).

[24] Cable/Home Communication Corp. v. Network Prods., Inc., 902 F.2d 829, 845-47 (11th Cir. 1990)

[25] Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. at 421, 435 n.17, 439. See also A&M Records, Inc. v. Abdallah, 948 F. Supp. 1449, 1456 (C.D. Cal. 1996), noting that Sony applies to cases involving "staple articles or commodities of commerce," such as VCRs, photocopiers, and blank, standard-length cassettes tapes. Contrast this with the finding in Napster II that it was sufficient that Napster knew that infringement was occurring, even though it was incapable of determining whether any particular file transfer constituted infringement. Opinion at 26-27.

recorder could not be held liable for the infringing acts of home consumers -- even though Sony knew consumers were using the VCRs to infringe copyright -- because the VCR could also be used for noninfringing "fair use" purposes such as to "time-shift" broadcast programming that consumers were invited to watch without charge, and to record programming where the copyright owner did not object.

Not every possible noninfringing use of a product may be considered "commercially significant." For example, the manufacturer of certain imported ROMless motherboards was held as a contributory copyright infringer where there was no evidence showing actual use of the motherboards with legitimate Apple ROM chips (rather than infringing ROM chip imports).[27] In Vault Corp. v. Quaid Software Ltd., the court of appeals affirmed that the producer of a software program designed to defeat Vault's anticopying computer software program, had not infringed Vault's copyright and was not contributorily liable for infringing use of its product by some customers, in light of the commercially significant noninfringing use of making permissible back-up and archival copies of the protected software. However, the court discounted the significance of other potential uses of the software that the defendant conceded had no commercial value.[28] Synthesizing these case principles, "commercial significance" or "substantiality" may be established if a consumer reasonably would acquire or use the product for the noninfringing purposes.

When evaluating noninfringing uses, courts will only look to noninfringing uses of those aspects of the products alleged to be put to infringing uses. For example, in Sony, the Supreme Court did not take into account the use of the VCR for playback purposes and, instead, evaluated only the noninfringing uses of the recording function of the product. Similarly, in Oak Industries, Inc. v. Zenith Electronics Corp.,[29] a court imposed contributory patent infringement liability where there were noninfringing uses

---

[26] Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. at 439.

[27] In re Certain Personal Computers and Components Thereof, Inv. No. 337-TA-140, 6 ITRD 1140, 1150 (1984).

[28] 847 F.2d 255, 263-64 and n.16 (5th Cir. 1988).

[29] 697 F. Supp. 988 (N.D. Ill. 1988)

for some elements of the accused product, but not for the particular aspects of the device that were alleged to infringe. The court distinguished this from the situation, such as in Sony, in which a device, to perform one function, necessarily but incidentally is capable of infringement.

Using Technology to Police Infringements

One mantra of content owners over the last decade is that "the answer to the problem of the machine lies in the machine." Technologies that regulate copying and redistribution can protect content through technological enforcement of individual compliance within the scope of behavior authorized by the copyright owner. In effect, technology can move the otherwise impossible task of enforcement against individuals one step higher in the chain, so as to place the burden upon the developers and manufacturers of recording and distribution technologies. Tasking technology companies and manufacturers with prevention of infringement therefore becomes an attractive option for an overall enforcement strategy.

However, the modest purpose of technological protection systems, to "keep honest people honest," acknowledges that even the most robust systems at some point will be defeated. Consequently, recent legislation mandates use of particular technologies and/or proscribes devices and actions that circumvent them. While intended to protect copyrighted works, such legislation regulates commerce rather than copyright. The result is a higher degree of protection for copyright owners, but less protection for the public interests that copyright was intended to serve, inasmuch as the explicit limitations and exemptions of copyright law, including fair use, do not apply to general commercial legislation.

The trend began with the Audio Home Recording Act of 1992, which required implementation in certain products of a simple system to prevent further digital copying of digital copies.[30] The Serial Copy Management System specifies two bits: one that signifies whether copy protection is being invoked over the content, and another that indicates whether the data is "original" or a "first generation" copy. The law imposes requirements in two technical areas.

---

[30] 17 U.S.C. § 1001, et seq.

- Devices that transmit and carry the content ("digital audio interface devices") must accurately carry or transcode the SCMS data, and not strip it.
- Recorders covered by the AHRA must read and respond to these codes. If the bits indicate that the incoming data has protection asserted and is "original," the recorder permits the making of a copy and marks it as a "first generation" copy. If the bits indicate that the incoming data has protection asserted and is already a first generation copy, the recorder prevents the making of a second generation or "serial" copy. Unlimited copies can be made from content where protection has not been asserted.

The AHRA has no exemption for fair use. It balances the technological protections for copyright owners with protections for consumers by "encoding rules" that ensure consumers the ability to make first generation copies from unencrypted compact discs and, in the future, digital radio broadcasts.[31] These compromise protections are a proxy for, rather than an implementation of, fair use, and thus imperfectly reflect through a binary "copy/no copy" choice some subset of the copying that might otherwise be sanctioned through a case-by-case weighing of multiple factors.

The battle resumed in 1995, with the issuance of the Report on Intellectual Property and the National Information Infrastructure, consummating with the 1998 passage of the DMCA. The DMCA presses copyright protection obligations upon technology companies in three ways.

- First, the DMCA proscribes services and technologies that circumvent access control systems such as encryption and authentication.[32]

---

[31] 17 U.S.C. § 1002(a) requires use of serial copy protections; § 1002(c) prohibits circumvention of the systems; and § 1002(d) proscribes intentional misencoding of original works so as to prevent copying.

[32] 17 U.S.C. § 1201(a) and (b). See also 17 U.S.C. § 114(d)(2)(C)(v)-(vii), imposing limited technological protection obligations on entities newly eligible for the statutory license to perform sound recordings.

Provisions clarify that this proscription applies to "self-enforcing" technologies such as would only be circumvented through intentional conduct, and does not mandate that device manufacturers affirmatively respond to these systems;[33] except that mandatory response is required to current analog video protection systems, balanced by encoding rules that impose limits on the types of content to which copy protection can be applied.[34]

- Second, the DMCA requires preservation of "copyright management information" (such as identifying watermarks) against intentional removal.[35]
- Third, Title II of the DMCA sets forth obligations that can be voluntarily adopted by an Internet service provider, online service provider or information location site; and, in return, obtain a "safe harbor" limitation of monetary and injunctive liability against allegations of contributory infringement.[36]

Like the AHRA, the DMCA has no exemption for fair use.[37] The few exemptions to these DMCA provisions, intended primarily to benefit research, archives and education, permit less personal copying and use than the AHRA.

---

[33] 17 U.S.C. § 1201(c)(3).

[34] 17 U.S.C. § 1201(k).

[35] 17 U.S.C. § 1202.

[36] 17 U.S.C. § 512.

[37] It is clear that 17 U.S.C. § 1201(c)(1) means that the DMCA does not diminish the fair use defense in cases alleging copyright infringement, not that fair use is a defense under § 1201(a) or (b) for users and manufacturers of circumvention devices. See Universal City Studios, Inc. v. Reimerdes, 00 Civ. 0277 (LAK) (S.D.N.Y.), Opinion, August 17, 2000 at 40-45 (stating that neither fair use nor the Sony standard applied to a case under Section 1201 of the DMCA involving the dissemination of unlicensed software to decrypt scrambled DVD movies). See also RealNetworks, Inc. v. Streambox, Inc., 000 U.S. Dist. LEXIS 1889 ¶¶ 15-16 (W.D. Wa. Jan. 18, 2000) (noting that devices that could be used for fair use, and thus be immune from liability under the Sony doctrine, are nevertheless liable under Section 1201 of the DMCA); and Statement of

As a result, digital media increasingly are being released in encrypted formats. CSS, the "Content Scrambling System" for DVD video was the first step in a copy protection chain. Data from a DVD or other digital video source will be encrypted for transmission between devices along a home network; recording devices will, again, encrypt the recorded data in other formats. DVD audio, and other media, will soon follow the same pattern of encrypted delivery, transmission and recording.

Watermarks also will assume a higher profile role in this new paradigm. The recording industry established late in 1998 the "Secure Digital Music Initiative" or "SDMI," which relies on watermarks initially to screen content so as to determine whether the content may be securely shared with devices that will respect the usage rules set by the content owner. In the video context, motion picture companies advocate use of watermarks for the dual purposes of "record control" – limiting or preventing the recording of watermarked content – and "playback control" – refusing to playback watermarked media that, but for the inevitable hacking of other protection mechanisms previously applied to the content, should not have been recorded. However, unlike the encryption and authentication systems protected under the DMCA, watermarks are not "self-enforcing." The requirement to read and respond to watermarks most efficiently can be imposed by legislation or licenses to other necessary technologies.[38]

Marybeth Peters, Register of Copyrights, before the House Subcommittee on Courts and Intellectual Property, on H.R. 2281, 105th Congress, 1st Session, September 16, 1997, at http://lcweb.loc.gov/copyright/docs/2180_stat.html

[38] On June 7, 2000, Disney Chairman and CEO Michael Eisner made this point in an address to the Joint Economic Committee of Congress:

> On offense, we ask you to begin to explore with us legislation that would assure the efficacy of technology solutions to copyright security. As we seek to develop measures such as watermarking, we need the assurance that the people who manufacture computers and the people who operate ISP's will cooperate by incorporating the technology to look for and respond to the watermarks. This same mandate could be part of the solution to a host of other Internet security issues as well.

http://www.senate.gov/~jec/eisner.htm

The Dilemma for Distributed Applications

Although users of distributed network applications may engage in direct infringement, the technology itself inherently remains neutral. Both the centralized and decentralized topologies operate exactly the same way regardless of whether all files being exchanged are authorized or unauthorized. At either extreme (all lawful/all unlawful), applying existing copyright law would be simple. The cases for distributed applications arise at points along a spectrum, and therein lies the dilemma.

The Dilemma of Imposing Vicarious Liability Upon Automatic Processes

With respect to vicarious liability, the dilemma is compounded by the different topologies described above for centralized and decentralized applications. For the decentralized "Gnutella" model, each participant along the network is both host and client. The right and ability to control user conduct resides only with the users themselves. As a result, vicarious liability for the acts of those who download is effectively inseparable from the direct act of authorizing the file for distribution. Enforcement for decentralized network applications therefore is identical to, and equally as problematic as, suing for direct infringement against each individual infringer. Hence, the concept of vicarious liability for decentralized distributed network applications has become irrelevant, if not entirely obsolete.

Centralized peer-to-peer systems, such as the "Napster" model, further test the vitality and extensibility of existing case law concerning vicarious liability. Some courts have suggested the possibility of vicarious liability where the technology could feasibly examine the exchanged data for indicia of permission.[39] However, in many cases the server responds to incoming requests in an automatic process, and has no actual ability to discern lawful from infringing conduct.

---

[39] See, e.g., Religious Tech. Center v. Netcom On-Line Communication Serv., Inc., in which the court declined summary judgment on a claim of vicarious infringement lodged against an Internet service provider, where the system users uploaded alleging material to the system using automatic and indiscriminate processes that operated without human intervention. The court found that the plaintiff had raised a question of fact whether Netcom could have exercised control by identifying and removing infringing postings to Usenet. 907 F. Supp. at 1375-76.

For the typical vicarious liability cases, cited above, the law developed around fact patterns in which physical contact and human intervention enabled the defendant to identify and remedy infringing conduct, whether it be supervising a store employee copying tapes or overseeing the goods sold at a flea market. In each case, the imposition of liability followed from the actual physical capacity for supervision by more than just an "absentee landlord."

For centralized systems, the server does perform an ongoing function in operating the system, hence the temptation exists to view service providers as more like the dance hall or swap meet operator. Yet the server's ability to exercise control may be limited and ineffective. If "control" translates as "the burden of screening all files," depending upon the nature and magnitude of the service this could be infeasible; or it could so engulf processing capacity as to degrade the system to an unacceptable level of performance. In this connection, in enacting "safe harbors" for service providers under the DMCA, Congress recognized that the impracticality or impossibility of screening data files justified limiting service provider liability for contributory or vicarious infringement allegations. While courts should be wary of creating new exemptions that Congress has declined to enact, the policies underlying the "safe harbor" provisions of the DMCA caution that the concept of "technological control" by automated systems may be more oxymoron than axiom.[40]

In any event, screening would likely be ineffective or futile for content that lacks indicia differentiating between authorized and infringing uses.[41] MP3 files cannot be

---

[40] In this connection, the court in Napster II held the Sony standard inapplicable because it concluded that Napster was a service, not a product. See Opinion at 24-25. The court's analysis contrasted the ongoing role of the Napster database and server with the role of Sony which ended at the point of purchase. Id. However, the service cases cited by the court involved situations involving continuing physical contact and personal supervision. To the extent that actual supervision becomes impossible using automated technical processes, it makes greater sense from a policy perspective to treat such systems as products rather than services; or, more to the point, to abandon the distinction between products and services and to focus the inquiry instead on the ability to exercise meaningful control.

[41] See Recording Indus. Assn. of America v. Diamond Multimedia Sys., Inc., 29 F. Supp. 624, 632 (C.D. Cal. 1998), *affd*, 180 F.3d 1072, 1078 (9th Cir. 1999) (noting that it would have been futile for a court, applying the AHRA, to require a handheld MP3

screened for copyright infringement, since the MP3 format lacks any "flags" or bits indicating whether copyright is being asserted over the material, or whether the copyright owner permits or objects to the exchange and reproduction of the sound recording. Moreover, any user can disguise the content by assigning an alternative name to the file. Hence, efforts to screen infringements using file names will be both overbroad and underinclusive. Such screening will miss works whose names have intentionally been changed to hide infringing popular music, but conversely will exclude files whose names have been intentionally changed to the names of popular songs or artists, so as to induce downloads of unknown artists. Further, screening by file name could eliminate access to different versions of the same song, or different songs with the same name, even though some of the affected copyright owners might not object to such access.

Therefore, in cases where the capacity to supervise is technologically infeasible or ineffective in sifting infringing from noninfringing acts, it seems unrealistic to ascribe to automated centralized servers the "right and ability to exercise control" over users, particularly where the data lacks copyright management information or other indicia of protection.[42] It is more likely that, with the trend toward technological protection mechanisms, vicarious liability will become a less potent weapon, and the norm for enforcement will be anticircumvention legislation.

---

player to implement the Serial Copy Management System inasmuch as MP3 files lack the necessary codes that indicate copyright status and copy status).

[42] The court in Napster II acknowledged Napster's argument that it is "technologically difficult, and perhaps infeasible to distinguish legal and illegal conduct." Opinion at 30. But, apparently referring to Napster's "blackballing" of more than 330,000 directly-infringing users identified by the band Metallica, the court concluded that Napster had the right and ability to supervise user conduct based on its ability to block individual users from access to the system. Opinion at 30. This seems erroneous in that it equates Napster's ability to respond after the fact with the ability to control in advance the individual uses. Only the latter should be relevant for purposes of finding the ability or right to control, otherwise defendants would always incur liability without the capacity to prevent it. Moreover, it would seem contrary to public policy to punish the centralized server for providing incomplete assistance to copyright owners where complete control is not possible. Under such circumstances, imposing liability might drive adoption of the decentralized model that cannot help copyright owners.

A Quantitative Approach to Contributory Infringement

With respect to contributory infringement claims, where products have both noninfringing and infringing uses, the courts must decide at which point the right to prevent unlawful activity outweighs the right to engage in legitimate conduct. The Supreme Court in the Sony decision enunciated a standard without drawing bright lines -- indeed, specifically declining to declare how much use is "commercially significant" -- effectively leaving quantification for future case-by-case analysis. 464 U.S. at 442.

Notwithstanding, at least two aspects of the Sony decision suggest that a quantitatively small usage can defeat a claim for contributory infringement. First, the Court drew its standard from its cases interpreting the patent statute providing for contributory infringement,[43] noting that imposing liability upon staple articles of commerce effectively extends the patent monopoly beyond the statutory grant, and that there is a public interest in access to products that can be used for noninfringing purposes. 464 U.S. at 440-441. The patent cases cited by the Court suggest that any commercial noninfringing use would be sufficient defense against liability.[44]

---

[43] "Whoever sells a component of a patented machine, manufacture, combination or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial noninfringing use, shall be liable as a contributory infringer."

35 U.S.C. § 271(c).

[44] "These cases deny the patentee any right to control the distribution of unpatented articles unless they are 'unsuited for any commercial noninfringing use.' Dawson Chemical Co. v. Rohm & Haas Co., 448 U.S. 176, 198 (1980). Unless a commodity 'has no use except through practice of the patented method,' id., at 199, the patentee has no right to claim that its distribution constitutes contributory infringement. … '[A] sale of an article which though adapted to an infringing use is also adapted to other and lawful uses, is not enough to make the seller a contributory infringer. Such a rule would block the wheels of commerce.' Henry v. A. B. Dick Co., 224 U.S. 1, 48 (1912), *overruled on other grounds*, Motion Picture Patents Co. v. Universal Film Mfg. Co., 243 U.S. 502, 517 (1917)."

Id. at 441-442.

Second, in applying the "capable of substantial noninfringing use" standard, the Sony Court found two independent and sufficient grounds for affirmance: (a) consumers could record programming that either was not copyrighted or whose owners did not object to the recording; and, (b) unauthorized time-shift recording for subsequent viewing was fair use. As to the first ground, the Court cited the district court finding that only some 7.3% of programming recorded by consumers fell into this category, id. at 424; yet, the Court held that imposing contributory liability would unfairly stifle the interests of those who welcomed time-shifting as a means to expand their audience. Id. at 446.[45]

Toward a New Mode of Analysis

Ultimately, "substantiality" or "commercial significance" should not be addressed solely as a quantitative inquiry. Quantitative analysis implicitly measures past or current usage. Moreover, a pure quantitative analysis ignores the public interests underlying

---

[45] "If there are millions of owners of VTR's who make copies of televised sports events, religious broadcasts, and educational programs such as Mister Rogers' Neighborhood, and if the proprietors of those programs welcome the practice, the business of supplying the equipment that makes such copying feasible should not be stifled simply because the equipment is used by some individuals to make unauthorized reproductions of respondents' works. The respondents do not represent a class composed of all copyright holders. Yet a finding of contributory infringement would inevitably frustrate the interests of broadcasters in reaching the portion of their audience that is available only through time-shifting.

"Of course, the fact that other copyright holders may welcome the practice of time-shifting does not mean that respondents should be deemed to have granted a license to copy their programs. Third- party conduct would be wholly irrelevant in an action for direct infringement of respondents' copyrights. But in an action for contributory infringement against the seller of copying equipment, the copyright holder may not prevail unless the relief that he seeks affects only his programs, or unless he speaks for virtually all copyright holders with an interest in the outcome. In this case, the record makes it perfectly clear that there are many important producers of national and local television programs who find nothing objectionable about the enlargement in the size of the television audience that results from the practice of time-shifting for private home use. The seller of the equipment that expands those producers' audiences cannot be a contributory infringer if, as is true in this case, it has had no direct involvement with any infringing activity."

Id., 464 U.S. at 446-447; footnote omitted.

copyright law, and in affording the public access to the means of engaging in noninfringing conduct.

The Supreme Court Sony standard, that a product need merely be "capable" of substantial noninfringing uses, suggests a more expansive assessment: current uses; the prospects for those current uses extrapolated into the future; and the potential emergence of new noninfringing uses. Thus, even a small but socially-valuable noninfringing use should be considered both for its current intrinsic importance and its potential impact should such use become widespread.

To address the capability of future noninfringing uses, therefore, the analysis also should encompass a qualitative examination of both the current and potential noninfringing uses. Such a qualitative inquiry more fully comports with the public and private interests implicated by intellectual property. As an example, the most fundamental public interest fostered by the grant of copyright is promoting the dissemination of copyrighted works. With reference to the above discussion of Sony, that public interest is fostered by file-sharing among interested consumers, but is outweighed by the impact of infringement to which all copyright owners object. Notwithstanding, as Sony suggests, this policy gains significance where copyright owners approve of or do not object to the dissemination.[46]

The public interest further extends to the progress and exploitation of new technology. From the printing press to the PC, technology is the means of bringing copyright works to the public. Inasmuch as one technological development may serve as building block for the next, a decision that bans new technologies -- especially ones as innovative as peer-to-peer networking software systems -- could have effects that reach much further than the case under consideration. Similarly, a proper analysis must also consider the impact of a decision upon the copyrights and patent rights of the manufacturers of products and software, since their independent rights to exploit their intellectual property could be negated by improvidently imposing contributory liability.

---

[46] One puzzling aspect of Napster II, then, is the court's failure to take cognizance of numerous copyright owners, including several gold and multiplatinum selling artists such as rapper Chuck D and the band The Offspring, who submitted affidavits indicating that they supported and did not object to the sharing of their works through Napster.

The following pages suggest a method for a evaluating third party liability for the manufacture and dissemination of new technologies that have both infringing and noninfringing uses, that takes into account both current analysis and these additional policies. These factors are not intended to be exclusive, nor the examples comprehensive. Rather, they illustrate the types of policies at issue when examining the existence and significance of noninfringing uses.

1. ***What is the nature of each potential noninfringing use?*** In evaluating the claims of infringement, courts describe the acts of infringement, their current impact upon copyright owners, and the potential impact of these acts should the infringing acts continue unabated. In ruling on third party liability claims, a court similarly should examine the character and value of the noninfringing uses of those particular aspects of the product used to commit the allegedly-infringing acts. In this regard, this inquiry echoes the first factor of the fair use analysis. As such, it is not a "test," but a first step in identifying the uses that will be evaluated in several of the factors below.

This examination should consider the intrinsic value of the uses to both the individual users (i.e., what benefit does the user derive from the use) and the owners of the material that is being used (e.g., what benefit is derived by copyright owners that do not object to the distribution or reproduction of their works). A court also should consider whether the uses have any ancillary beneficial effects, such as whether the uses implement legitimate facilities provided for by law (e.g., the backup copying of software at issue in Vault v. Quaid), or create socially valuable structures (e.g., communication among admirers of particular art forms or artists, or among advocates of particular socio-political points of view). However, courts should resist giving weight to only the types of journalistic, educational or scientific purposes enumerated in the fair use statute,[47] inasmuch as the Sony decision finds that even copying of entertainment programming in its entirety can be deemed a fair and protected use.

Importantly, the Sony standard -- being "capable" of substantial noninfringing uses -- requires courts to focus beyond the current extent of existing uses. The inquiry encompasses both the potential extent of existing uses in the future, and new potential

---

[47] 17 U.S.C. § 107.

uses as well. In this latter connection, courts should attempt to extrapolate new potential uses based on current uses of the technology and on analogous acts accomplished by other means. For example, if lending or exchange of physical objects today is commonplace, a court safely could presume that these practices would also become commonplace for digitized files.

Such analysis requires reasoned foresight, and admittedly it is easy for subjective preconceptions to cloud objective judgments. Yet, today's products often become popular for surprising and initially unintended purposes. Few among us could accurately have predicted the pervasive role in daily life of facsimile machines, cell phones, laptop and palm-top computers, personal music players and recorders or the World Wide Web. The inevitable myopia of the present-day counsels caution in how we envision our cohabitation with technology even two or five years hence.

Applying this factor, then, the greater the potential intrinsic value of a noninfringing use, the greater the care that must be taken not to stifle or preclude that use by banning the technology.

2. ***What is the likelihood that any consumer would acquire and use the product for these noninfringing purposes?*** As noted, current case law deems a use "insubstantial" if it is unlikely that the public actually would employ the accused technology for that purpose. Thus, noninfringing uses may be "substantial" as a matter of law if a significant number of persons would engage in those uses at least some of the time.

A lawsuit would not be brought if all persons used the product for noninfringing purposes all the time, and might not be seriously contested if all persons used the product for infringing purposes all the time. Thus, the purpose of this factor is to assess where the evidence lies along a spectrum of how many users engage in noninfringing conduct for what percentage of the time.

As discussed under factor 1 above, quantification of existing uses is but one element of this analysis. Evidence suggesting quantification of potential uses also should be considered (e.g., by reference to sales and penetration rates for analogous technologies and services). Moreover, a court should attempt to qualitatively evaluate these existing

and potential uses, so as to assure that intrinsically valuable uses will receive due consideration.

Under this factor, if the evidence suggests a number of existing or potential noninfringing uses whose uses are not insubstantial, or the existence of intrinsically valuable noninfringing uses that would be fostered by the technology, then this factor should weigh against a finding of third party liability.

3. ***What is the role of the technology in facilitating the infringing uses?***

This factor addresses whether the technology facilitates previously unknown means of infringement, or whether there alternative means have been available to commit the same acts of infringement. The court should consider whether there is a genuine difference in the magnitude of infringement using the various means, or whether the difference lies in the efficiency of infringement. For example, the mere existence of other means of infringement should not justify the existence of another or more efficient means. Notwithstanding, an increase in infringement or efficiency might be outweighed by other factors.

4. ***What is the role of the technology in facilitating the noninfringing uses?***

The Sony decision was founded explicitly upon the public interests implicated in the availability of noninfringing uses of the technology. Thus, in reviewing claims for third party liability, a court also must consider how the technology facilitates such uses. Does the technology enhance the means by which the public accesses or uses copyrighted works for noninfringing purposes? Does the availability of such technology induce more copyright owners to make their works available for such licensed or unobjectionable uses? Does the technology otherwise increase the efficiency of disseminating copyrighted works for such noninfringing uses? For example, does the accused technology facilitate provide an easier interface; improve file compression size, performance characteristics or transmission speeds; or expand the database of works available for noninfringing uses?

Under this factor, a manufacturer should be able to establish a need for the technology if there are no alternate or equivalent access to noninfringing uses, or if the technology meaningfully increases public access to noninfringing uses. A showing of

need, coupled with intrinsically valuable noninfringing uses, would support a finding of no contributory infringement.

5. ***What is the likelihood that, if the technology is or is not deemed to be infringing, that noninfringing uses will proliferate?*** Fair use analysis considers the potential harm to the copyright owner should the alleged infringement become widespread. The factor suggested here essentially inverts that fair use factor, to assess the impact of the technology in facilitating future noninfringing uses. It is based upon the same premise underlying factor 4, i.e., that a technology that may substantially expand noninfringing uses has greater entitlement to a favorable judgment than a technology that has no perceptible impact on noninfringing use.

Courts therefore should consider the extent to which the technology makes possible the noninfringing uses, and whether previous means to achieve the noninfringing uses are equally efficient and equally accessible to the public as the technology at issue. Similarly, a court should consider whether a finding of infringement would compel the technology owner to eliminate certain product capabilities and, as a result, reduce the capacity for certain noninfringing uses. In such cases, a court should consider the impact on noninfringing uses if the technology were altered so as to accommodate the interests of aggrieved copyright owners. For example, if a music sharing program would be required to be redesigned so as to accept only encrypted content, a court could evaluate the potential harm to any new and established artists that wished to disseminate their music in unprotected formats.

6. ***What impact would a finding of infringement have upon the technology and technological progress?*** This factor evaluates the public interest in the availability of the technology. Consideration should be given to whether hindering current uses of this technology might also impede development and use of the technology for other purposes. For example, a court might assess whether or how a finding of infringement with respect to the sharing and copying of music might deter development of similar technology for other unprotected media, such as photographs or text, or for protected media. In balancing these factors, a court should hesitate to impose liability where such a finding might impede the use of the technology for other noninfringing purposes.

Conclusion

Copyright ultimately serves a public purpose. When public and private interests collide, the public interests emerge as paramount.[48] For that reason, this paper suggests factors that reflect the public policies underlying copyright and third party liability, and the public interests in securing access both to noninfringing uses of copyrighted works and to technologies that facilitate these and future noninfringing uses.

Courts face a difficult task in balancing public and private interests, and we cannot expect omniscience in their decisionmaking. Nevertheless, the interests of all parties can only be protected with careful analysis and reasoned foresight. Particularly when evaluating evolutionary technologies such as peer-to-peer network applications, the risks facing copyright owners, technology companies and the public at large are genuine and complex. Copyright owners bear tremendous financial risk from widespread infringement that may be facilitated by such technologies, and restraining technology can provide more direct, effective and efficient enforcement than the courts. Yet, imposing constraints on technology can kill the goose that lays the golden egg. The same technology that facilitates infringement often creates new markets for copyright owners, and socially-beneficial opportunities for consumers.

It bears repeating that the VCR navigated a to remain tortuous path through the courts to the retail shelf. In 1976, the movie studios sued for contributory copyright infringement. A district court first found for Sony, but the court of appeals then reversed, in favor of the plaintiff movie studios. More than seven years after suit was filed, the Supreme Court found for Sony -- after two oral arguments, and by only a single vote.[49] How different our world would be today without the VCR and the technologies it spawned -- such as digital audio tape recorders and digital video cassette recorders (that

---

[48] "The immediate effect of our copyright law is to secure a fair return for an author's creative labor. But the ultimate aim is, by this incentive, to stimulate artistic creativity for the general public good. 'The sole interest of the United States and the primary object in conferring the monopoly,' this Court has said, 'lie in the general benefits derived by the public from the labors of authors.'" Twentieth Century Music Corp. v. Aiken, 422 U.S. 151, 156 (1975); citations and footnotes omitted.

[49] See "Betamax: The Inside Story," http://www.hrrc.org/html/inside_betamax.html

use the same helical-scan recording head technology), and DVD and DVD recorders (built upon the existing consumer appetite for home video). How different will our world be tomorrow if the courts deal Internet technologies, like distributed network applications, a different fate?