

Copyright's Digital Dilemma Today: Fair Use or Unfair Constraints? Part I: The Battle over File Sharing

by Lee S. Strickland

Editor's note: This article has been split into two parts. The first covers the legal controversy over file sharing. The second, to be published in the December/January 2004 issue of the *Bulletin*, covers other critical developments in e-copying.

Lee S. Strickland, J.D., is visiting professor in the College of Information Studies, University of Maryland; e-mail: LSTRICKL@deans.umd.edu

In previous issues we surveyed some of the critical legal and policy developments in the world of records and information management (*Bulletin*, June/July and August/September 2003) – a key concern for every business whether directly focused on the task of homeland security or more generally contributing to our national economic interests. Today we continue our survey of cutting-edge developments of interest to information professionals with a focus on the most current intellectual property issues – the ultimate business asset in our information age. As with our previous articles, we also provide recommendations for management steps as well as additional research and sources for maintaining currency in this rapidly developing arena. *Especially critical for every business and every individual is our discussion of potential and almost certain liability for infringement given the proliferation of peer-to-peer (P2P) network connections in the corporate environment and among home users.*

The Contest Over Intellectual Property Rights

Twenty-five years ago, perhaps even 10 years ago, intellectual property law in general and copyright law in particular were of importance to information professionals but were relatively static from legal and policy perspectives. But more recently, our information age and information economy have propelled this subject to extreme importance and exponential change – in large part because technology has vastly altered the medium of intellectual property. The result has been efforts by millions to gain access to intellectual property on their

terms – such as unauthorized electronic sharing of copyrighted music – and, in response, by business to protect their content by increasingly aggressive tactics.

In response to these drivers, the Computer Science and Telecommunications Board (CTSB) of the National Academies of Science issued its seminal report in 2000 – *The Digital Dilemma: Intellectual Property in the Information Age*. The study was predicated on the truism that the very technologies underlying the information age and providing extraordinary levels of access to information were also greatly enhancing infringement. As a result, the CTSB concluded that our current intellectual property laws – developed in the physical world of paper and tangible goods – simply did not work well in the digital world. Although the CTSB offered many thoughtful proposals, the approach of content providers has changed little. Indeed positions appear to have hardened with industry demanding greater control in a multiplicity of ways and users fearing that traditional fair use concepts will be eroded if not eliminated. And thrust into this contest were the courts and the Congress as they have struggled to address this tsunami of transformation.

As information professionals, we have a primary responsibility for understanding these rapid developments and shaping the underlying policy debates. For example, how has the electronic environment changed the basics of established copyright law? Should it? How is the Digital Millennium Copyright Act (DMCA) being used – as expected by Congress or in unforeseen ways? What are the

rules for public domain today for published and unpublished materials since the Supreme Court has now upheld the Copyright Term Extension Act. And what does the TEACH Act mean for me? These are some of the many questions we will explore.

E-Copying — New Technology Does Not Change Established Law

Where previously there were photocopy machines and singleton copies there is now electronic reproduction with unlimited copies. But from a legal perspective, electronic copying is simply traditional infringement with new tools, and a number of litigations have confirmed that cyberspace does not change traditional law. The most visible case evidencing this truism was *A&M Records, et al. v. Napster*, filed in December of 1999 in federal court in San Francisco by a number of record companies against the Internet company that provided a frequently used search tool for locating MP3 music files on the PCs of other, individual Internet users. As we know the defendant did not itself provide or host music files and the suit was therefore based on the allegation that its service facilitated copyright infringement and that it was therefore liable under the established doctrine of contributory infringement.

Initially, on July 26, 2000, following detailed hearings and consideration, the district court granted a preliminary injunction on the grounds that consumers who use Napster service and software to exchange sound files containing copyrighted musical recordings are engaged in direct copyright infringement and that Napster itself is liable for contributory infringement as well as vicarious infringement. However, two days later, the U.S. Court of Appeals for the 9th Circuit granted a stay nine hours before Napster was to shut down – finding that Napster’s appeal “*raised substantial questions (on) both the merits and the form of the injunction*” and setting a schedule for expedited consideration. That followed in October 2000 with, generally considered, critical questions posed to the record industry lawyers. At the same time, the U.S. Copyright Office filed an amicus brief arguing, in part, that the Audio Home Recording Act was not a relevant defense.

But predictions of decisions based on factors such as critical questioning by appellate judges are notoriously unreliable – on February 12, 2001, the 9th Circuit affirmed the decision of the trial court framing the following issues and holdings and providing us important guidance for the future.

Is there direct infringement by the individual users of Napster or do they have a valid defense such as fair use? The answer was direct infringement given the four statutory fair use factors. First, as to “purpose and character of the use,” the copying was not transformative and was commercial in nature given the scope and objective (i.e., “to save the expense of purchasing the authorized copies”). As to “nature of the use,” the works are creative and thus closest to core protection and furthest from a finding of fair use. As to “portion of use,” the

works were copies *en toto* and in massive or “wholesale” quantities. And as to “effect of use on market,” there was material impact given expert testimony; and, in any event, a lack of harm to an established market is not the only issue since harm can come from preventing plaintiffs’ development of a secondary electronic market for their goods.

If the individual users are liable, then is Napster liable under a theory of contributory infringement or vicarious infringement? The answer was “yes” to both questions. First, contributory infringement requires a finding of “...*knowledge of the infringing activity and personal conduct that encourages or assists the infringement.*” Here, Napster had both actual and constructive knowledge that its users exchanged copyrighted music. Moreover, the *Sony* decision is of no use given Napster’s actual specific knowledge; the *Sony* court had refused only to impute knowledge given the potential of the equipment to infringe. Second, vicarious infringement requires a finding of “...*the right and ability to supervise the infringing activity and also a direct financial interest in such activities.*” Here, Napster has the ability and authority to block infringers but only a limited ability to identify copyrighted information – it does not read the contents of the MP3 files and can identify copyrighted material only by the “titles” as listed by its users. It also has a financial interest since the infringing material “acts as a draw.” Given the limits on Napster’s ability to identify infringing material – and the equal ability of the copyright holders to do so – the Court found that this ground required modification of the injunction to require identification by the copyright holders but then to require resolute remedial action by Napster.

Does the Audio Home Recording Act apply to this case? The answer was “no” inasmuch as computer hard drives are not defined in the Act as “*digital audio recording devices*” and the MP3 recordings on computer hard drives are not defined as “*digital music recordings.*”

Does “sampling” and “space (or time) shifting” by individual users constitute fair use? Here the court found these arguments not only unavailing but inapplicable. Specifically, “sampling” is in essence “promotional downloads” which is a tightly regulated activity by the plaintiffs generating substantial royalties from the process; hence, the free sampling would not constitute fair use. And, the shifting argument (relying on the *Rio* and *Sony* cases) was similarly inapplicable since this case did not involve an individual user moving a file legally owned or acquired from one place to another but rather involved massive distribution of copyrighted material to the general public.

Lastly, are the affirmative defenses of waiver, implied license and copyright misuse applicable? Again, the answer was “no.” Just because the music industry has promoted MP3 technology for legal purposes does not mean that it has waived its intellectual property interests, including its authority to exer-

cise exclusive control over the creation and distribution of MP3 files of its music.

In conclusion, the 9th Circuit found infringement on the part of Napster but remanded only to require the plaintiffs to provide notice to Napster of copyrighted works and files prefatory to Napster's burden and duty of disabling access to the offending content. And, without question, the Court reiterated that Napster bore the burden of policing its system within the technical and practical limits of that system. In relatively quick succession, an injunction followed in March 2001 requiring both parties to take action to identify and remove infringing materials, the company voluntarily took down its servers to attempt compliance and the company failed in its efforts to re-invent itself as a subscription-based, pay-for-download service despite an abortive partnership and later sale to German media giant Bertelsmann AG.

The Stage Shifts – Decentralization

With the demise of Napster, a bevy of new music-trading software products emerged (e.g., Aimster, Kazaa and Morpheus) that were based on a true peer-to-peer architecture with no central control and no central index. Here, when

A technology note: The P2P network is not truly index-free – rather the software distributing company (and most visible litigation target) does not maintain any index or specific knowledge of traded content. In fact, the index responsibility is assigned to certain users. More specifically, any Kazaa user having a broadband connection will be designated a “supernode” and will thus automatically maintain a list of some of the files (and IP addresses) made available by other Kazaa users, usually on the same Internet Service Provider (ISP) network. When a given Kazaa user initiates a search, the software first queries the nearest supernode and it provides immediate results; that first supernode then refers the search to other supernodes (and so forth) as necessary. The actual file sharing takes place directly between the requesting PC and the target PC – not through the supernode and not the software company. As is evident, every member of the Kazaa network that functions as a supernode quite arguably has the same legal liability as Napster for contributory infringement. And, of course, every individual user is similarly and potentially liable for direct or contributory infringement depending on whether that user is downloading or simply making available a copyrighted work.

users download the software, they become members of this network and can share files directly with other members – whether those files are innocent family photographs or copyrighted music. And, as might be expected, the recording and movie industry lost no time in bringing federal lawsuits against Aimster (later renamed Madster) in Chicago and Morpheus (and others) in Los Angeles.

But there were legal problems based on the technology at issue – couldn't these services more clearly claim the *Sony* defense since they had no knowledge of and control over individual trading? Remember that in *Sony*, the Supreme Court held that the sale of VCRs did not constitute contributory infringement even though Sony knew in general that the machines could be used and perhaps were being used to infringe copyright. This was because the VCRs were capable of both infringing and “substantial noninfringing uses” and the fact of generic or constructive knowledge of infringing activity was insufficient to give rise to liability given only the sale of the devices. The clear holding was that the mere sale of items in commerce does not constitute a civil wrong if the items are capable of appropriate uses. Indeed the courts have often used the analogy of “sexy lingerie and prostitution” to explain the logic underlying this decision.

In any event, the cases moved forward to very recent fruition. First came the *Aimster* litigation by the Recording Industry Association of America (RIAA) and the P2P service was shut down in short order by the U.S. District Court in Chicago on a preliminary injunction pending trial. And that decision was promptly upheld in July by the U.S. Court of Appeals for the 7th Circuit. Why was this so clear despite the *Sony* defense? Quite simply, Aimster suffered from their bravura and was quite unable to demonstrate any legal issues of their service as stated by the appeals court: “*Far from doing anything to discourage repeat infringers of the plaintiffs’ copyrights, Aimster invited them to do so, showed them how they could do so with ease using its system and by teaching its users how to encrypt their unlawful distribution of copyrighted materials, disabled itself from doing anything to prevent infringement.*”

But between the two decisions in *Aimster* came the *Grokster/Morpheus* decision based on summary judgment arguments in December 2002. In a decision that surprised many, given the string of industry victories to date, the trial court on April 25, 2003, ruled in favor of two of the defendants – Grokster and StreamCast Networks (distributor of Morpheus) – finding no direct, contributory or vicarious liability based on the defendants’ lack of control of individual users and the fact that the software had valid non-infringing uses. In other words, the arguments based on the 1984 U.S. Supreme Court decision involving the *Sony Betamax* had won the day.

How could this be? How could the *Sony* defense win and lose seemingly identical cases? Quite simply, it was a matter of a better defense and better proof. Here, the defendants were

able to establish that there were substantial noninfringing uses for their software: distributing movie trailers, free songs and other non-copyrighted works including Shakespearean plays, government documents and other public domain materials.

But this is not to suggest that the story ends here. The RIAA responded testily that “[b]usinesses that intentionally facilitate massive piracy should not be able to evade responsibility for their actions” and has appealed the decision, although success in the Court of Appeals is doubtful given the thoughtful, fact-based nature of the decision. What is significant in the strategic sense is the observation of the trial court that it is not “blind to the possibility that Defendants may have intentionally structured their businesses to avoid secondary liability for copyright infringement, while benefiting financially from the illicit draw of their wares... [and that]...additional legislative guidance may be well-counseled.” As we shall see, it appears certain that the music industry will continue the fight at both the individual and the Congressional level.

Resource notes: The primary decisions concerning technology and the liability for direct or contributory infringement are:

- *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984).
- *A&M Records, et al., v. Napster*, 239 F.3d 1004 (9th Cir. 2001)
- *MGM Studios v. Grokster*, 2003 U.S. Dist. LEXIS 6994 (C.D. Cal. 25 April 2003)
- *In re Aimster Copyright Infringement*, 2003 U.S. App. LEXIS 13229 (7th Cir. 30 June 2003)

Decentralized Sharing and Innocent Service Providers

Given the demise of Napster and the rise of decentralized sharing, industry attention has also focused on service providers that provide the connectivity for P2P users. One favorable feature of the DMCA (section 512(c)(1)) was the limitations of liability for service providers otherwise known as the “safe harbor” provisions – a significant step given past cases that had held service providers liable for vicarious infringement under the 1976 Copyright Act. In general it provides a defense from copyright liability for typical operations if the provider (1) has rules to prohibit infringement and to terminate repeat offenders, (2) has no knowledge of infringement, (3) does not interfere with any technical schemes to protect copyright data and (4) acts expeditiously to remedy infringement upon notice. This protection however is dependent upon registration with the U.S. Copyright Office (USCO) and the adoption of a set of policies that regulate user activ-

ities (e.g., acceptable use policy) as well as specific “take down” and “put back” policies that guide activities when a notice of infringement is received including required notice to the individual. It is important to note that the definition of service provider is very broad – any entity providing online services or network access – and clearly could encompass every public or private business today, including, of course, libraries and educational institutions.

The U.S. Naval Academy (USNA) is case in point. Last November, in response to RIAA demands, authorities seized nearly 100 student computers suspected of containing copyright-protected content. This issue is bedeviling college administrators across the country where students have the benefit of broadband Internet connections and where the copyright industry is well aware and well focused on this threat. Critical to continued immunity is the adoption of computer policies that prohibit students from utilizing the institutional network to access and transmit copyrighted content and to penalize offenders (e.g., immediate termination of use).

Three final factoids of importance are the extent of the demands and the research that must be accomplished before such demands are made by copyright holders and resulting action by service providers. First, it appears that the USNA action was initiated as part of a mass effort by the recording and movie industry to over 2,000 colleges and universities – an effort that continues today and has an increasing focus. Second, the factual predicate to such demands is very low – perhaps good news for content providers and service providers but bad news for alleged offenders. According to a very recent decision in *Motion Picture Association of America (MPAA) vs. InternetMovies.com* by the U.S. District Court in Hawaii, the DMCA requires no investigation before asserting a take-down notice even if the claim is unresearched and/or inaccurate. And third, the DMCA immunities provision also precludes a lawsuit against the service provider by the individual alleged to be responsible for the infringing material – a not insignificant point in this litigious age.

A practice note: The fee to register for the DMCA immunity is currently \$30.00 and the forms are available online at the following addresses:

- www.copyright.gov/onlinesp/agent.pdf (for initial designation)
- www.copyright.gov/onlinesp/agenta.pdf (for amendments).

The Battle Shifts to Individuals

Little more than a year ago, §512 of the Digital Millennium Copyright Act (DMCA) was a little-noted provision but harbored potentially great power: it allowed for automatic issuance of subpoenas in DMCA cases without any judicial

consideration. Today, the RIAA and Verizon have made this section a feared weapon in the copyright wars.

Here is the story. After crushing the visible, big infringers such as Napster, it was expected that the RIAA would begin to move against individual alleged violators – especially, as we considered previously, technology moved toward P2P. But how could the music industry find allegedly infringing material on individual's machines? The answer is part technical, part guesswork and part legal. The industry finds content it deems infringing the same way that you find music that you want to copy (i.e., internet-shared folders on your machine). The industry identifies the content as copyright-protected by guesswork (i.e., the designated file name appears "close enough" to their copyright catalog). And the industry identifies the name and address of individuals offering or downloading that content through a §512 subpoena to their ISP. The legal and policy issue? These subpoenas are issued by the music company itself, without any pending litigation, without any showing of necessity or violation of law, without any judicial review and without any right of the target to contest the matter.

In short order, the RIAA issued numerous subpoenas and much to the credit of Verizon (in its role as an ISP), the company refused to release the demanded customer data. RIAA thereafter filed a motion in the U.S. District Court for the District of Columbia to enforce compliance in October of 2002. Unfortunately, individual rights were the loser: first, on January 22, 2003, the court rejected Verizon's statutory challenges based on the fact that the RIAA's subpoena related to material transmitted over Verizon's network (rather than stored on it) and thus fell outside the scope of the subpoena power authorized by §512(h). And second on April 24, 2003, the court also rejected Verizon's constitutional claims based on the argument that the subpoena power violates Article III of the Constitution (because it authorizes federal courts to issue binding process in the absence of a pending case or controversy) as well as the First Amendment rights of Internet users. A week later, the D.C. Circuit Court of Appeals refused a stay, thus requiring immediate compliance by Verizon of the release the names and addresses.

A Risk Assessment for Networks and Individuals

The risk posed by the recording industry to individuals trading copyrighted content – as well as corporate entities that provide connectivity to employees, students and others – is substantial and real. It is substantial in terms of civil and criminal penalties. Civil remedies for copyright infringement may include *actual damages* or *statutory damages* – an alternative form of recovery since actual damages may be difficult to prove or limited in dollar amount in typical cases. Statutory damages are specified in three categories for each single infringement of a single work: *normal* with damages from \$750 to \$30,000; *willful* with damages increasing to \$150,000; and *innocent* with a court allowed to reduce damages to an

amount not less than \$200. Clearly the stage is being set to obviate any claim of innocent infringement and impose willful penalties. Moreover, criminal penalties for individuals are also a real risk especially given the passage of the No Electronic Theft (NET) Act, an amendment in 1997 that removed the personal financial gain or commercial advantage element and provides for penalties that include up to five years in prison and/or \$250,000 fines and a statute of limitations extended from three to five years.

And it is real in terms of the extent of infringement and the clear actions underway by the industry. Although a substantive appeal of the Verizon litigation was to be heard in September 2003 by the Court of Appeals, the wheels of litigation against individuals began almost immediately – on June 26 the RIAA announced publicly that they were "*preparing a wave of civil lawsuits against people who use music-trading software.*" Targeting would include the public directories of peer-to-peer providers and according to privacy advocates at the Electronic Privacy Information Center (EPIC), some 57 million Americans could be liable to these "*dinosaurs [that] have completely lost touch with reality.*" As of late July and reported by the *Washington Post*, over 1,000 such subpoenas had been issued with a rate of at least 75 additional per day.

The corporate environment – from private businesses to educational institutions – is no different. According to a very recent survey by AssetMatrix, a Canadian network monitoring company, as reported by CNET News.com, the installation of P2P clients in corporate environments is more than common – it is pervasive. While this would be expected in education, it is somewhat of a surprise in private industry. The study considered over 500 companies of varying size and found that every company of 500 or more employees had at least one installation of Kazaa or similar sharing software. The president of AssetMatrix was cogent in his observation: "*Corporations are frantic about how to rein in some control over this. Like with software licenses, most companies want to be on the right side of the law. The challenge is how they do that.*" As with the effort against educational institutions, the focus of copyright holders and the legal liability of corporations are certain – last year, the RIAA settled a copyright claim against Integrated Information Systems for \$1 million. At that time the senior vice president for the RIAA noted: "*This sends a clear message that there are consequences if companies allow their resources to further copyright infringement.*" In the most recent action (July 2), the RIAA served a DMCA subpoena on DePaul University in Chicago. This action presents the very practical issue of what quantity of offending material will trigger RIAA action. While the RIAA has previously suggested that they will target only "*substantial collections,*" the DePaul action appears to involve a user with only a handful of potentially infringing files.

In the next issue we will continue our survey of current intellectual property developments.