



Criminal Prosecution of On-Line "File Sharing"

by

**Joseph D. Schleimer, Esq.
& Kenneth D. Freundlich, Esq.**

Journal of Internet Law, August, 2001

(This article was originally presented by Kenneth D. Freundlich at the Harvard Law School, Berkman Center for Internet & Society on May 18, 2001)

Since Napster went on line, literally *billions* of music copyright infringements have been funneled through its "peer-to-peer" architecture. Seeking to exploit a perceived loophole in the Copyright Act, the operators of Napster built a massive user base by giving away other people's music, but as of yet the company has only managed to inflict damage on the copyright owners -- without making a profit for itself.

Inspired by Napster, the so-called "file sharing" web sites have proliferated rapidly, and along the way they have promulgated a crypto-libertarian/internet philosophy, preaching to an entire generation of gullible young fans that "music should be free."

The legal system has been slow to respond to this tidal wave of copyright infringements, and new "decentralized" systems such as Gnutella threaten to place the phenomenon beyond the control of the Courts. However, for the cynical venture capitalists and internet freebooters who continue to promote on-line "file sharing" systems there may be a surprise in store: *criminal indictment* under the "No Electronic Theft" ("NET") Act of 1997.

This article discusses the legal, technological, and doctrinal obstacles to the criminal prosecution of "file sharing" under the NET Act.

A. United States v. LaMacchia and the NET Act

The NET Act was a legislative response to *United States v. LaMacchia*, 871 F. Supp. 535, 545 (D. Mass. 1994). In that case, David LaMacchia, an MIT student, used the University's computers to create a bulletin board where users could post -- and download -- copyrighted software such as WordPerfect and Excel. Millions of dollars worth of software was distributed for free, and the worldwide traffic generated by Mr. LaMacchia's operation soon caught the attention of MIT officials, who reported him to the Justice Department.

After the indictment, Mr. LaMacchia's lawyers moved to dismiss on the grounds that the copyright statute, as it existed at that time, required a *profit motive* to prosecute copyright infringement as a crime. Since Mr. LaMacchia had set up his software "sharing" bulletin board as a stunt, and never intended to financially profit from the resulting free-for-all, no crime had been committed -- despite the huge monetary loss suffered by the copyright owners.

In his opinion dismissing the charges against LaMacchia, U.S. District Court Judge Richard G. Stearns expressed great displeasure with the gap in the law which the Defendant was slipping through, and recommended legislative reform:

"This is not, of course, to suggest that there is anything edifying about what LaMacchia is alleged to have done. If the indictment is to be believed, one might at best describe his actions as heedlessly irresponsible, and at worst as nihilistic, self-indulgent, and lacking in any fundamental sense of values. Criminal as well as civil penalties should probably attach to willful, multiple infringements of copyrighted software even absent a commercial motive on the part of the infringer. One can envision ways that the copyright law could be modified to permit such prosecution."

The NET Act of 1997 was Congress' direct and immediate response to Judge Stearns' admonition.

The legislative history of the Act discusses the compression of music files using the MP3 technology and describes it as a looming threat, so there is no question that the statute was specifically intended to criminalize the use of so-called "file sharing" systems to swap copyrighted music on line. In fact, one member of Congress argued in favor of the NET Act legislation by prophetically warning that "[w]e cannot allow the Internet to become the Home Shoplifting Network."

The thrust of the NET Act was to lower the standard for *mens rea* in copyright infringement prosecutions by eliminating the requirement to prove a profit motive. In place of the pre-LaMacchia standard, the Act created two separate methods for proof of the *scienter* element of the crime:

First, the NET Act imposed criminal penalties if the infringer is merely hoping

for a financial gain. The statute then defines "financial gain" as the "receipt, or expectation of receipt, of anything of value, *including the receipt of other copyrighted works.*" 17 U.S.C. Sections 101, 506(a)(1)(Emphasis added).

The Napster system falls squarely within this definition because it operates by automatically scanning the user's hard drive, posting the user's music files on the Napster index, and making them available for uploading by other users, at the exact moment the user logs onto the system with the expectation of downloading free music. Thus, the Napster system involves the exact kind of *quid pro quo* which the NET Act outlaws.

In other words, Napster is involving its millions of users in conduct which is, arguably, a *per se* criminal violation of the Copyright Act. By downloading, the Napster user is infringing the exclusive right of reproduction; by uploading, he or she is infringing the exclusive right of distribution. 17 U.S.C. Sections 106(1), (3); *Playboy Enterprises, Inc. v. Webbworld, Inc.*, 991 F.Supp. 543 (N.D. Tex. 1997).

Under the NET Act, the "exchange" aspect of the Napster transaction, if willful and knowing, is a criminal act. Under the RICO statute, participants in groups formed for the purpose of illegal "file sharing" could, potentially, also be charged as members of a racketeering enterprise. 17 U.S.C. Section 506(a); 18 U.S.C. Sections 1961, 2319.

Second, the NET Act includes an alternate *mens rea* formulation for cases like LaMacchia, where the operator facilitates voluminous file-sharing infringements without any expectation of personal gain *at all*. Thus, under 17 U.S.C. Section 506(a)(2), it is criminal to willfully infringe a copyright:

"[B]y the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than \$1000...."

At the current retail price for singles, the willful "file sharing" of as few as 150-170 songs during a six-month period could be charged as a Federal misdemeanor, carrying a potential one-year sentence and \$100,000 fine. 17 U.S.C. Section 506(a)(2); 18 U.S.C. Sections 2319(b)(3), 2319(c)(3), 3571(b)(5).

If the user uploads and downloads an aggregation of music with a retail value in excess of \$2,500 during a six-month period (approximately 400 to 450 songs at current retail prices), the infringement can be charged as a *felony*, including the possibility of a three or five-year jail sentence and a fine up to \$250,000. 18 U.S.C. Sections 2319(b)(1), 2319(c)(1)(e), 3571(b)(3).

B. The "Safe Harbor" Provisions of the Digital Millenium Copyright Act

Napster was financed by ultra-sophisticated Silicon Valley venture capitalists, who developed a base of more than *seventy million* (70,000,000) users at "warp speed" by giving away literally *billions* of copies of other people's music. From the outset, Napster had intellectual property lawyers on board, who believed they could operate their piratical system under the cover of the "safe harbor" provisions of the Digital Millenium Copyright Act ("DMCA").

The *immunity* provisions of the DMCA were enacted in 1998, to shield internet "service providers" from lawsuits based on copyright infringements *by their customers*. The Napster system sought to slip through this perceived loophole, by linking users seeking music with other users who have the music on their hard drive.

Napster operates through the use of a search engine, index and dialog box. The downloader enters the name of a recording artist into the dialog box, which conducts a Boolean search and locates the desired music on the C drive of another user. An index of available selections appears on the screen, and the downloader clicks on the desired music. Napster then connects the downloader and uploader together, and the actual exchange of the infringed music file takes place between the two users, over the Internet, outside of the Napster system.

Thus, Napster is doing *exactly* what Mr. LaMacchia did -- joining together uploaders and downloaders of copyrighted material for the purpose of infringement. The only meaningful difference is one of scale: Mr. LaMacchia's bulletin board operation enabled at most a few hundred copyright infringements. Napster has already arranged for, encouraged and facilitated *billions* of infringements.

Under the applicable "safe harbor" provision of the DMCA, 17 U.S.C. Section 512(d), an internet service provider is immune for linking together copyright infringing users *only* if the service provider acts *without knowledge of the infringement*. In the civil lawsuit, Napster's safe harbor defense was quickly stripped away by the RIAA's litigation attorneys, who used aggressive discovery to prove that Napster's executives *knew full well* that their system was being used to infringe copyrighted music. Indeed, the evidence which emerged demonstrated that is exactly what Napster was *designed* to do. In one damaging exhibit from the case, a co-founder of Napster wrote:

"Users will understand that they are improving their experience by providing information about their tastes without linking that information to a name or address or other sensitive data that might endanger them (especially since they are exchanging pirated music)."

Napster sought to build a mass user base by brazenly *touting* its service as the world's largest source of MP3 files -- and promising users they could find their "favorite music" without having to plow through "page after page of unknown artists."

Napster executives also admitted, in deposition, that they had used the system to beef up their *personal* music libraries, by downloading copyrighted music without paying for it.

As the RIAA's attorneys put it in their brief to the U.S. Court of Appeals for the Ninth Circuit:

"The ability to download myriad music files without payment seems to constitute the glittering object that attracts Napster's financially-valuable user base....Every day, Napster enables, encourages and directly benefits from the infringement of *12 to 30 million* copyrighted works."

Napster's DMCA defense was quickly rejected by the U.S. District Court, which granted a preliminary injunction in the civil proceeding and labeled Napster a piracy operation. *A&M Records, Inc. v. Napster, Inc.*, 114 F.Supp.2d 896, 927 (N.D.Ca. 2000). After initially staying the preliminary injunction, the Ninth Circuit affirmed, but ordered modifications. *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001).

Napster's last-ditch defense under the DMCA is based on the "notice and take down" provisions of the Act. Napster claims it can still benefit from DMCA immunity if it complies with those provisions. This defense assumes that "actual knowledge" is irrelevant, and presumes that immunity exists *unless and until* the copyright owner gives formal notice of infringing materials on the peer-to-peer system. Napster also relies on a clause in the DMCA whereunder the notice must include "identification of the reference or link" leading to the infringing material. 17 U.S.C. Section 512(d)(3).

Thus, Napster has claimed it only has to block music on the system which has been identified by the copyright owner *by file name*.

File names for the same song differ from user to user. As a result, blocking particular file names on Napster does not block posting of the music under a different file name. With tens of millions of users logging onto the system, the Napster postings evolve minute by minute, so Napster can block one set of user files, but the next batch of users can quickly re-post the blocked musical works under slightly different file names.

The result is the Napster "filename shuffle." As an illustration, on the date this article is being completed (May 16, 2001), it has been three months since the Ninth Circuit determined that Napster should be enjoined and more than two months since the injunction was issued. On this date, Napster is ostensibly blocking the copying of music by Aerosmith. However, a multitude of songs by Aerosmith can still be downloaded through Napster -- merely by inserting a space into the filename, i.e., typing "Aero smith" into the Napster dialog box.

On this date, Napster is also blocking files which use the name "ZZ TOP," correctly including a space. Napster is not, however, blocking files which spell "ZZTOP" without the space -- and the result is that scores of ZZ TOP recordings are still available for illegal downloading through Napster. (This, even though the authors of this article sent a "cease and desist" letter to Napster, on ZZ TOP's behalf, several months ago.)

As a result of using the "filename shuffle," on today's date (May 16, 2001), the Napster web site is also illegally offering up music by Elton John, Billy Joel, Van Morrison, Frank Sinatra, Miles Davis, Jimi Hendrix, Janis Joplin, Bruce Springsteen, Don Henley, James Taylor, Sheryl Crow, Pink Floyd, Led Zeppelin, Def Leppard, The Police, the Bee Gees, the Dixie Chicks, Garth Brooks, Tim McGraw, Faith Hill, Jennifer Lopez, Destiny's Child, the Backstreet Boys, and Matchbox 20.

The reader should note that the foregoing artists are mentioned merely as an *illustration*; virtually every major recording artist of recent decades is still available through Napster on May 16, 2001 -- notwithstanding a Federal injunction requiring Napster to cease and desist which has been in effect *more than two months*.

In a *criminal* prosecution for copyright infringement, the government bears the burden of proving every single element of a *civil* copyright infringement, in addition to proof of criminal intent. See, e.g., *United States v. Wise*, 550 F.2d 1180, 1190 (9th Cir. 1977). Thus, a successful civil defense based on the DMCA "safe harbor" provision would defeat a criminal prosecution based on the same facts.

However, the United States Court of Appeals for the Fourth Circuit has considered -- and flatly rejected -- the argument that compliance with the notice-and-take-down provision requires the copyright owner to give a precise list of file names. The Fourth Circuit also unequivocally rejected the argument that complying with the notice-and-take-down procedure immunizes a service provider which had *actual or constructive knowledge* of the infringement.

In *ALS Scan, Inc. v. Remarq Communities, Inc.*, 239 F.3d 619, 623 (4th Cir., 2001), the Court of Appeals held:

"[T]o qualify for this safe harbor protection [under the DMCA], the Internet service provider must demonstrate that it has met all three of the safe harbor requirements, and a showing under the first prong -- the lack of actual or constructive knowledge -- is prior to and separate from the showings that must be made under the second and third prongs...."

The Court analyzed the legislative history of the DMCA, and further explained its reasoning as follows:

"The DMCA was enacted both to preserve copyright enforcement on the Internet and to provide immunity to service providers from copyright infringement liability for 'passive,' 'automatic,' actions in which a service provider's system engages through a technological process initiated by another without the knowledge of the provider. H.R. Conf. Rep. No. 105-796, at 72 (1998)....This immunity, however, is not presumptive, but granted only to 'innocent' service providers who can prove they do not have actual or constructive knowledge of the infringement....The DMCA's protection of an innocent service provider disappears at the moment the service provider loses its innocence...."

The "innocence" requirement for services which link infringing users together (17 U.S.C. Section 512(d)) was specifically discussed in the Senate Judiciary Committee Report on the DMCA, No. 105-190 (105th Cong., 2d Sess.) at p.48:

"Section 512(d) provides a safe harbor that would limit the liability of a service provider that refers or links users to an online location containing infringing material....Like the information storage safe harbor in section 512(c), a service provider would qualify for this safe harbor if, among other requirements, it 'does not have actual knowledge that the material or activity is infringing' or, in the absence of such actual knowledge, it is 'not aware of facts or circumstances from which infringing activity is apparent.' *Under this standard, a service provider would have no obligation to seek out copyright infringement, but it would not qualify for the safe harbor if it had turned a blind eye to 'red flags' of obvious infringement.* For instance, the copyright owner could show the provider was aware of facts from which infringing activity was apparent if the copyright owner could prove that the location was clearly...a 'pirate' site...where sound recordings, software, movies or books were available for unauthorized downloading, public performance or display." (Emphasis added)

The Judiciary Committee Report made it clear that Congress sought only to protect "innocent" technology companies from liability for conduct by their customers -- not eviscerate the NET Act by creating a loophole for blatant, LaMacchia-style "file sharing" infringers.

C. Aimster

Napster has inspired a plethora of imitators, some of which employ wink-and-a-nod euphemisms in explaining the purpose of their service. For example, where

Napster got itself in deep trouble by openly touting the availability of free music, the operators of "Aimster" have been much cagier, offering only to assist the user in finding internet "buddies" with "similar interests."

The Aimster "screen shot" shows a sample dialog box in which the user has typed "audi" and has found a "buddy" with a file available for downloading containing "car sounds."

Sub silentio, the message is clear: You can use Aimster to get "car sounds" if you want to, but you can also use it to get free music, just like Napster.

On the advice of its lawyers, Aimster was careful to avoid making public statements that its *purpose and intent* was to enable file-sharing of copyrighted works. If it had adhered to such a strategy, it would have been much more likely to succeed with a DMCA defense, or a First Amendment defense, or a "mere technology" defense under *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984).

However, Aimster's overly-exuberant executives undermined the entire strategy when they impulsively developed and released (in the space of a few hours) the notorious "Pig Encoder" software.

The Pig Encoder was a special program which had as its sole function the scrambling of music filenames using Pig Latin. Thus, the Pig Encoder would assign a file name to a Madonna song by scrambling her name to read "adonnaM."

The Pig Encoder was designed and released by Aimster executives for the express, sole and singular purpose of subverting the preliminary injunction in the Napster case. See, *Reuters*, March 6, 2001, "Aimster Says Pig Latin Code Can Circumvent Napster Injunction."

The Pig Encoder was short lived: Under intense pressure, Aimster took it down after a little more than one week. See, *Fox Market Wire*, March 15, 2001, "Aimster Pulls Pig Latin Encoder."

Thus, the real accomplishment of the Pig Encoder was to strip away the facade of Aimster's "innocent intent" defense, and reveal the company for what it really is: A Napster copy-cat, making a desperate attempt to build an internet business through "file-sharing" copyright infringements.

D. Gnutella

Gnutella operates without a central server, relying on a series of transactions whereby file-sharing users locate each other by daisy-chaining from one "small" server/index to the next, until the desired musical material is located. Along the way, the user's computer generates an ever-expanding list of URL addresses where music or other copyrighted material can be uploaded and downloaded for free, from other

Gnutella users.

Gnutella-type decentralized file sharing systems deprive the copyright owners of a stationary, corporate target to sue or prosecute. Ultimately, to combat Gnutella (and Gnutella imitators), copyright owners are going to have to legally engage the *individual* uploaders and downloaders. Publicized criminal prosecutions under the NET Act are one possible way of doing that.

On a related topic, see: "[Electronic Countermeasures Against Copyright Infringement on the Internet: The Law and Technology](#)," by Joseph D. Schleimer, Esq.

[HOME](#)