Electronic Frontier Foundation

IAAL*: What Peer-to-Peer Developers Need to Know about Copyright Law

by Fred von Lohmann
Senior Intellectual Property Attorney
Electronic Frontier Foundation
fred@eff.org

v. 5.0, January 2006

I. What this is, and who should read it.

The future of peer-to-peer file-sharing is entwined, for better or worse, with copyright law. Copyright owners have already targeted not only the makers of file-sharing clients like Napster, Scour, Audiogalaxy, Aimster and Kazaa, and Morpheus, but also companies that provide products that rely on or add value to public P2P networks, such as MP3Board.com, which provided a web-based search interface for the gnutella network. The U.S. Supreme Court in *MGM v. Grokster* addressed some, but by no means all, of the copyright law issues that may confront P2P developers and other technologists in the future.

If these courtroom skirmishes yield any lesson for P2P developers, it is that a legal strategy needs to be in place early, preferably at the beginning of development, rather than bolted on at the end.

This piece is meant as a general explanation of the U.S. copyright law principles most relevant to P2P file-sharing technologies. It is aimed primarily at:

- Developers of core P2P file-sharing technology, such as the underlying protocols, platform tools, and specific client implementations; and
- Developers of ancillary services that depend upon or add value to P2P file-sharing networks, such as providers of search, security, metadata aggregation, and other services.

The following discussion is meant as a general introduction, and thus glosses over many of copyright law's more subtle nuances. It is aimed not at giving you all the answers, but rather at allowing you to recognize the right questions to ask.

What this is not: The following discussion focuses only on U.S. copyright law, and does not address any issues that may arise under non-U.S. law. While non-copyright principles may also be mentioned, this discussion does not attempt to examine other legal principles that might apply to P2P file-sharing, including patent, trademark, trade secret, or unfair competition. Nothing contained herein constitutes legal advice—please discuss your individual situation with your own attorney.

II. Overview

This paper is divided into four sections:

---

* Acronym for "I am a lawyer," to distinguish from the common "IANAL" ("I am not a lawyer") that appears on Slashdot and other online forums. This white paper was originally titled "IAAL: Peer-to-Peer File Sharing and Copyright Law after Napster."

- An introduction to basic copyright concepts and terminology, including the three most relevant forms of copyright liability for P2P developers—contributory infringement, vicarious liability, and inducement.
- A review of the chief P2P cases decided to date—*Napster, Aimster,* and *Grokster.*
- An overview of the chief defenses that may be available to P2P developers.
- Ten specific things P2P developers can do that may reduce the risk of copyright infringement liability.

III. Copyright basics and the intersection with P2P file sharing.

Copyright law applies to virtually every form of expression that can be captured (or, to use the copyright term of art, "fixed") in a tangible medium, such as on paper, film, magnetic tape, hard drive, optical media, or (arguably) in RAM. Songs, books, photographs, software, and movies are all familiar examples of copyrighted works. Copyright law reserves certain rights exclusively to the owner of the copyright, including the rights to reproduce, distribute, and publicly perform the work.

The nature of file-sharing technology inevitably implicates copyright law. First, since most digital files are "fixed" for purposes of copyright law (whether on a hard drive, CD, or possibly in RAM), the files being shared generally qualify as copyrighted works. Second, the transmission of a file from one person to another generally results in a reproduction. Copyright owners have also argued that digital transmissions can qualify as a distribution, and possibly a public performance (in the world of copyright law, "public performance" may include the act of transmitting a copyrighted work).

Thus, to a copyright lawyer, every reproduction, distribution, and public performance requires an explanation, and thus file-sharing seems suspicious from the outset.

A. The end-users: "direct" infringement.

For the individuals who are sharing files, the question becomes whether all of these reproductions, distributions, and public performances are authorized by the copyright owner or otherwise permitted under copyright law (as "fair use," for example). So, if the files you are sharing with your friends are videos you took of your vacation, you are the copyright owner and have presumably authorized the reproduction, distribution, and performance of the videos.

However, if you are sharing MP3's of Metallica's greatest hits, or disc images of the latest Microsoft Office install CD, the issue becomes more complicated. In that case, assuming that the copyright owner has not authorized the activity, the question of copyright infringement will depend whether you can qualify for any of the limited exceptions to the copyright owner's exclusive rights. If not, you're what copyright lawyers call a "direct infringer"—you have directly violated one or more of the copyright owner's exclusive rights.

In a widely-used public P2P file-sharing environment, it is a virtual certainty that at least some end-users are engaged in infringing activity (unless the application is specifically designed not to function as a general purpose networking tool, but instead to permit only certain "authorized" files to be shared). When the major record labels and music publishers decided to sue Napster, for example, it was not difficult for them to locate a large number of Napster users who were sharing copyrighted music without authorization.

B. The P2P tool maker: secondary infringement.

But what does this have to do with those who develop and distribute peer-to-peer file-sharing tools? After all, in a pure P2P file-sharing system, the vendor of the file-sharing tool has no direct involvement in the copying or transmission of the files being shared. These activities are handled directly between end-users.

Copyright law, however, can sometimes reach beyond the direct infringer to those who were only indirectly involved in the infringing activity. As in many other areas of the law (think of the "wheel man" in a stick up, or supplying a gun to someone you know is going to commit a crime), copyright law will sometimes hold one individual accountable for the actions of another. So, for example, if a swap meet owner rents space to a vendor with the knowledge that the vendor sells counterfeit CDs, the swap meet owner can be held liable for infringement alongside the vendor.

Under copyright law, this indirect, or "secondary," liability can take three distinct forms: **inducement**, **contributory infringement** and **vicarious liability**.

1. Inducement.

In its June 2005 ruling in *MGM v. Grokster*, 125 S.Ct. 2764 (2005), the Supreme Court announced a new form of secondary liability, which it described this way:

> "[O]ne who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties."

In other words, in order to prevail on an inducement theory, a copyright owner must prove each of the following elements:

- **Direct Infringement**: There has been a direct infringement by someone.
- **Affirmative Act**: The accused inducer has made statements or taken other active steps directed at encouraging infringing uses. Examples of affirmative steps may include advertising a product for infringing uses, instructing users how to infringe (including when providing customer support), or anything else that "entices or persuades" a user to commit infringement. It can also include promotional efforts aimed at deliberately attracting infringers to use your product (e.g., trying to attract the users of the old Napster service).
- **Intent**: The accused inducer intended to promote copyright infringement. Courts generally allow intent to be shown by circumstantial evidence, which means that copyright owners will argue that almost anything could be relevant to establishing what the defendant intended. For example, copyright owners may point to how a company makes money, whether it could have modified its software to reduce infringing uses, and whether it was trying to attract infringers as users. As part of the litigation process known as "discovery," copyright owners may be entitled to search through company and individual emails and other documents, as well as interview potential witnesses under oath, in order to develop evidence of intent.

2. Contributory infringement.

Contributory infringement is similar to "aiding and abetting" liability: one who knowingly contributes to another's infringement may be held accountable. Or, as the courts have put it, "one who, with knowledge of the infringing activity, induces, causes, or materially contributes to the infringing conduct of another, may be held liable as a contributory infringer."[1]

So, in order to prevail on a contributory infringement theory, a copyright owner must prove each of the following elements:

- **Direct Infringement**: There has been a direct infringement by someone.
- **Knowledge**: The accused contributory infringer knew of the underlying direct infringement. This element can be satisfied by showing either that the contributory infringer actually knew about the infringing activity, or that he reasonably should have known given all the facts and circumstances. At a minimum, however, the contributory infringer must have some specific information about infringing activity—the mere fact that the system is capable of being used for infringement, by itself, is not enough.
- **Material Contribution**: The accused contributory infringer caused or materially contributed to the underlying direct infringement. Merely providing the "site and facilities" that make the direct infringement possible can be enough. Copyright owners have argued that simply providing software or a device that makes infringement possible is "material contribution."

Holding technology developers responsible for the unlawful acts of end-users obviously can impose a crushing legal burden on those who make general-purpose tools. Fortunately, the Supreme Court has defined an outer limit to contributory infringement.

In *Sony v. Universal City Studios*, 464 U.S. 417 (1984), a case brought by the movie industry against the Sony Betamax VCR, the Supreme Court found that contributory infringement liability could not reach the manufacturer of a device that is "capable of substantial noninfringing use." In that case, the Court found that the VCR was capable of several noninfringing uses, including the time-shifting of television broadcasts by home viewers. Rather than focusing on the *proportion* of the uses are noninfringing, the Supreme Court adopted a standard that asks whether the technology is "merely capable" of substantial noninfringing uses.

The "*Betamax* defense" has been under sustained legal attack in cases involving P2P technology. In the *Napster* case, for example, the court found that this defense, even if effective against a contributory infringement claim, will not protect a defendant from a vicarious liability claim (discussed below). In the *Aimster* case, the court suggested that the *Betamax* defense may require an evaluation of the proportion of infringing to noninfringing uses, contrary to language in the Supreme Court's *Sony* ruling.

---

[1] In the wake of the Supreme Court's decision in *MGM v. Grokster*, discussed in more detail below, it is not clear whether this traditional formulation of contributory infringement has been replaced, or merely supplemented, by the Supreme Court's newly announced "inducement" approach. Until this question is resolved in the courts, the prudent course of action would be to avoid any conduct that would give rise to liability under *either* the newly announced inducement theory or the traditional formulation of contributory infringement.

The Supreme Court in *MGM v. Grokster* did little to clarify the debates surrounding the *Betamax* defense. Instead, the Court based its ruling on an inducement theory and made it clear that the *Betamax* defense does not apply to inducement.

The heart of the debate, still unresolved, is whether the *Betamax* defense turns on a product's "capability" or "primary use." The entertainment industry continues to argue that anyone who continues to distribute a product, knowing that it is primarily used for infringement, is a contributory infringer, notwithstanding the *Betamax* defense. The technology industry disagrees, arguing that so long as your product is "merely capable" of substantial noninfringing uses, it does not matter what the proportion of infringing or noninfringing uses might turn out to be.

In short, the law surrounding the *Betamax* defense remains in flux, putting P2P developers (and all technologists) on unpredictable legal ground when it comes to contributory infringement.

3. Vicarious liability.

Vicarious liability is derived from the same legal principle that holds an employer responsible for the actions of its employees. Vicarious liability applies where a defendant has the right and ability to supervise the direct infringer and also has a direct financial interest in the infringer's activities.

Thus, in order to prevail on a vicarious liability theory, a copyright owner must prove each of the following:

- **Direct Infringement**: There has been a direct infringement by someone.
- **Right and Ability to Control**: The accused vicarious infringer had the right and ability to control or supervise the underlying direct infringement. This element does not necessarily set a high hurdle. For example, the *Napster* court found that the ability to terminate user accounts or block user access to the system was enough to constitute "control."
- **Direct Financial Benefit**: The accused vicarious infringer derived a "direct financial benefit" from the underlying direct infringement. In applying this rule, however, the courts have not insisted that the benefit be especially "direct" or "financial"—almost any benefit seems to be enough. For example, the *Napster* court found that "financial benefit exists where the availability of infringing material acts as a draw for customers" and the growing user base, in turn, makes the company more attractive to investors.

The nature of vicarious liability creates a strong incentive to monitor the conduct of your users. This stems from the fact that knowledge is not required for vicarious liability; a person can be vicariously liable even if she is completely unaware of the underlying infringing activity.

As a result, if you exercise control over your users and derive a benefit from their activities, you remain ignorant of their conduct at your own risk. In the words of the *Napster* court, "the right to police must be exercised to the fullest extent. Turning a blind eye to detectable acts of infringement for the sake of profit gives rise to liability." In addition, the court in *Napster* declared that the *Betamax* defense is not applicable to vicarious liability claims. Accordingly, if you have control over, and derive a financial benefit from, direct infringement,

the existence of "substantial noninfringing uses" for your service is irrelevant (at least in the Ninth Circuit, which covers most of the western U.S., where *Napster* was decided).

The entertainment industry has argued that the failure to implement "filtering" technologies (i.e., technologies that are able to identify content as not authorized for sharing) should be enough to establish "control" for purposes of vicarious liability. In other words, if you could redesign your technology so as to control or reduce infringing uses, but fail to do so, you should be vicariously liable. No court has yet accepted this argument, although the Supreme Court in *MGM v. Grokster* noted that the failure to add filtering could be evidence of "intent" in connection with an inducement claim.

IV. Indirect liability and P2P file sharing: the cases so far.

As of August 2005, there have been three major court opinions that have applied indirect liability theories to companies that distribute P2P software:

A&M Records v. Napster, 239 F.3d 1004 (9th Cir. 2001)

In re Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003)

MGM v. Grokster, 125 S.Ct. 2764 (2005)

Unfortunately, these three cases are not entirely consistent in their analyses. The law continues to evolve, and other courts may further muddy the waters in the years to come.

A. The *Napster* case.

In the *Napster* case, the music industry plaintiffs admitted that Napster did not, itself, make or distribute any of their copyrighted works. Instead, they pressed contributory infringement and vicarious liability theories. Based on these theories, the plaintiffs convinced a federal district court to grant a preliminary injunction against Napster. The injunction was appealed and affirmed by the Ninth Circuit Court of Appeals in February 2001 (Napster ultimately declared bankruptcy and was liquidated before any final ruling on liability).

Turning first to contributory infringement, the Ninth Circuit upheld the lower court's findings:

- **Direct Infringement**: At least some Napster users are direct infringers, because they distributed and reproduced copyrighted music without authorization.
- **Knowledge**: Napster had actual knowledge of infringing activity, based on internal company emails and the list of 12,000 infringing files provided by the RIAA. Moreover, Napster should have known of the infringing activity, based on the recording industry experience and downloading habits of its executives and the appearance of well-known song titles in certain promotional screen shots used by Napster.
- **Material Contribution**: Napster provided the "site and facilities" for the directly infringing conduct of its users.
- ***Betamax* Defense Rejected**: Although the court admitted that Napster was capable of substantial noninfringing uses, it ultimately found the *Betamax* defense inapplicable because Napster had *actual knowledge* of *specific infringing material* and *failed to block access or remove* the material. In the Ninth Circuit's view, that was enough to overcome the *Betamax* defense.

The Ninth Circuit also endorsed the lower court's vicarious liability analysis:

- **Direct Infringement**: At least some Napster users are direct infringers, because they distributed and reproduced copyrighted music without authorization.
- **Right and Ability to Control**: Napster has the ability to control the infringing activity of its users because it retains the right to block a user's ability to access its system.
- **Financial Benefit**: Napster derived a financial benefit from the infringing activities of its users because this activity acted as a "draw" for customers, and a portion of Napster's value is derived from the size of its user base.

The Ninth Circuit concluded, however, that the lower court had not adequately considered the technological limits of the Napster system when crafting the preliminary injunction. In ordering the district court to revise its injunction, the Ninth Circuit spelled out some guiding principles. First, in order to prevent contributory infringement, Napster was required to take reasonable steps to prevent further sharing of music *after receiving notice* from a copyright owner that a particular recording is being shared on its system without authorization. Ultimately, Napster voluntarily implemented a number of filtering mechanisms (including file name filters and acoustic fingerprinting filters) intended to filter out works that were not approved for sharing. These filters were never accurate enough to satisfy the district court judge, and Napster ended up in bankruptcy before a trial could be held.

Second, in order to stave off vicarious liability, the Ninth Circuit declared that "Napster…should bear the burden of policing its system within the limits of the system." During the period until its bankruptcy, Napster and the plaintiffs bitterly disagreed about what these monitoring obligations entailed. At a minimum, Napster had the duty to terminate users who were identified as infringers. Beyond that, there was little agreement. The disagreement was never fully resolved by the court, since Napster was shut down while it worked on improving its filtering technologies.

B. The *Aimster* case.

In the *Aimster* case, the music industry plaintiffs made the same vicarious and contributory infringement claims that they did in the *Napster* case. They succeeded in obtaining a preliminary injunction that ultimately shut Aimster down pending the trial on the merits (like Napster, Aimster went bankrupt before a trial could occur). In June 2003, the Seventh Circuit Court of Appeals upheld the preliminary injunction ruling.

In upholding the preliminary injunction, the appeals court relied solely on the contributory infringement claim. The court did not engage in the traditional contributory infringement analysis, instead engaging in a more general discussion of several relevant concepts, including the *Betamax* defense. In the end, the court upheld the injunction because Aimster had (1) failed to introduce *any* evidence of noninfringing uses and (2) had engaged in activities that demonstrated clear knowledge of infringing activities.

With respect to the issue of knowledge, the court focused on "tutorials" that specifically encouraged Aimster users to download popular copyrighted music. The court also was not impressed by the fact that Aimster network traffic was encrypted, allegedly making it impossible for Aimster to know exactly what files were being shared by individual end-users. In the eyes of the court, the steps taken by Aimster to avoid knowledge supported an inference of "willful

blindness." (This suggests that, at least in some courts, copyright owners may argue that you "knew" what your users were up to, even if encryption makes it impossible for you to monitor their activities; this makes the *Betamax* defense even more critical with respect to contributory infringement.)

Turning to the *Betamax* defense, the court concluded that Aimster had failed to introduce *any* evidence that the Aimster software had ever been used for anything other than infringing activity. This finding alone was enough to disqualify Aimster from relying on the *Betamax* defense (which requires a showing that the technology in question is at least capable of a substantial noninfringing use).

The court, however, went on to suggest that application of the *Betamax* defense requires a consideration of the *proportion* of the infringing to noninfringing uses. This is in direct conflict with language contained in the Supreme Court's opinion in the *Betamax* case. The discussion of proportionality in the *Aimster* opinion is arguably not binding on any subsequent court, as the outcome in that case was determined by Aimster's failure to introduce *any* evidence of noninfringing uses for its technology. In any event, the *Aimster* ruling simply underscores the continuing controversy over whether the proportion of infringing and noninfringing uses is relevant to the *Betamax* defense.

C. The *Grokster* case.

The *MGM v. Grokster* case involves three sets of defendants—the makers of the Kazaa, Morpheus and Grokster P2P file sharing software. Unlike the software at issue in the *Napster* and *Aimster* cases, the software here was decentralized in nature—once the software was downloaded and installed by a user, the software vendors had no ability to monitor or control what it was used for, nor did the software vendors maintain any central indexes or bootstrap servers. Two of the defendants, Grokster and StreamCast Networks, succeeded in getting the lawsuit as to at least some versions of their software thrown out, a ruling that was later affirmed by the appellate court, but reversed by the Supreme Court.

Although the entertainment industry plaintiffs originally argued that the defendants were liable for contributory infringement and vicarious liability, the Supreme Court in June 2005 found that there was enough evidence on inducement to justify a trial and thus reversed the lower courts. The Supreme Court did not resolve the contributory infringement or vicarious liability questions posed in the case, but sent those questions back for the lower courts to address.

As discussed above, the Supreme Court announced a new theory of copyright inducement liability:

> "[O]ne who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties."

The Supreme Court began its analysis by stating that the *Betamax* defense, whatever its scope, does not apply to inducement claims. In the words of the Court, "where evidence goes beyond a product's characteristics or the knowledge that it may be put to infringing uses, and shows statements or actions directed to promoting infringement, [the *Betamax* defense] will not preclude liability." (In two concurring opinions, the Justices split 3-3 on their interpretation of the proper scope of the *Betamax* defense as applied to the traditional theories of contributory infringement and vicarious liability.)

According to the Supreme Court, inducement requires both an "affirmative act" and "intent" on the part of the defendants to foster infringing uses. The Court pointed to three things that it believed might constitute an "affirmative act" for inducement purposes:

- Advertisements aimed at attracting Napster users to use defendants' OpenNap servers (an earlier technology that pre-dated the decentralized P2P software distributed later);
- Newsletters that contained links to news articles that discussed infringing uses of the software; and
- Customer support messages responding to users who were having trouble locating or playing copyrighted materials.

This list of examples should be viewed as merely illustrative—the Court specifically cautioned that other kinds of activities might satisfy the "affirmative act" requirement in other cases.

The Court pointed to the following things it felt could be relevant to the question of "intent":

- Internal communications and advertising designs that indicated a purpose of bringing about infringing acts;
- Efforts to attract former Napster users ("a known source of demand for copyright infringement");
- Failure to implement filtering or other mechanisms to diminish infringing activity; and
- A business model premised on advertising that yielded increased revenues as overall usage of the software increased.

In *MGM v. Grokster*, the Supreme Court concluded that there was enough to permit the entertainment industries to go forward with their case, and therefore set aside the lower court rulings in favor of StreamCast and Grokster, sending the case back to the district court in Los Angeles for a trial or other further proceedings.

In the final analysis, by disposing of *MGM v. Grokster* on inducement grounds, the Supreme Court missed an opportunity to clarify the traditional secondary liability doctrines of contributory infringement and vicarious liability. As a result, software developers are left to puzzle their way through the uncertainties and contradictions left by the *Sony*, *Napster* and *Aimster* rulings, as well as any future rulings by the lower courts in *MGM v. Grokster*.

V. Potential defenses against secondary liability claims.

A. No direct infringer: "All of my users are innocent."

If there is no direct infringement, there can be no indirect liability. Consequently, if no users in the network are sharing copyrighted works without authorization, this would be a complete defense to any inducement, contributory infringement, or vicarious liability claims. Unfortunately, this may be extremely difficult to demonstrate, given the decentralized nature of most P2P networks and the wide variety of uses to which they may be put. Even if file sharing by some users is privileged under the "fair use" doctrine or another statutory exception to copyright, it will be very difficult to show that *every* use falls within such an exception. Nevertheless, in certain specialized "walled garden" networks that permit the sharing of only secure, authorized file types, this may be a viable defense.

B. The *Betamax* defense: "Capable of substantial noninfringing uses."

As discussed above, the Supreme Court concluded in *Sony v. Universal* that contributory infringement liability could not reach the manufacturer of a device, so long as the device is "capable of substantial noninfringing use."

Unfortunately, the "*Betamax* defense" has been under sustained legal attack in cases involving P2P technology. The various rulings have not always been consistent, creating considerable ambiguity. But all three of the major court rulings—*Napster, Aimster,* and *Grokster*—make it clear that developing a clear record of substantial noninfringing uses is critically important for software developers who fear they may be sued for contributory infringement.

There remain many unsettled questions, however. First, it is unclear whether the *Betamax* defense applies to both contributory infringement and vicarious liability claims, or only against the former. The Ninth Circuit in *Napster* limited the defense to contributory infringement claims, but a different court outside the Ninth Circuit might rule otherwise. In addition, there is still some question about whether the proportion of infringing and noninfringing uses can be a relevant factor in applying the *Betamax* defense. The two concurring opinions in *MGM v. Grokster* take different views on this, but each opinion only attracted the votes of 3 Justices of the Supreme Court, shy of the majority required to clarify the law. The *Aimster* decision, meanwhile, says that an examination of proportion is important, but does so in what lawyers call "dicta" (i.e., discussion was not necessary to the outcome of the case, and thus is entitled to less weight).

The conflicting court interpretations of the *Betamax* defense have at least two important implications for P2P developers. First, they underscore the threat of vicarious liability—at least in the Ninth Circuit, a court will not be interested in hearing about your "substantial noninfringing uses" if you are defending against a vicarious liability claim. Accordingly, "control" and "direct financial benefit," as described above, should be given a wide berth. This will likely reduce the attractiveness of business models built on an on-going "service" or "community-building" model, to the extent that these models allow the provider to control user activity (i.e., terminate or block users) and create value by attracting a large user base.

Second, with respect to contributory infringement, the lower court rulings in *Grokster* suggest that a technology vendor may be better off with designs that confer no ability to control user activities after the software has been downloaded and installed. After all, once you receive specific notices from copyright owners about infringing activities, courts may be tempted to wonder why you did not "do something" about the infringing activities (e.g., the Supreme Court recognized this as potentially relevant to showing a defendant's "intent" for purposes of inducement). In that context, the scope of your obligation may depend on the extent that the architecture allows you to "do something." In cases involving truly decentralized P2P networks built on open source software, there may be nothing a software developer or vendor can do to stop infringing activities (just as Xerox cannot control what a photocopier is used for after it is sold). To the extent you want to minimize your obligation to police the activities of end-users, this counsels strongly in favor of software architectures that leave you with no ability to control, disable, or influence end-user behavior once the software has been shipped to the end-user.

Copyright owners have recently begun arguing that technologists have a duty to *redesign* technologies (e.g., by implementing "filtering" mechanisms) once they are put on notice

regarding infringing end-users. This argument has never been accepted by the courts. However, future developments are difficult to predict. Breaking developments on this front may have important ramifications for P2P developers and should be closely monitored.

C. The DMCA Section 512 "safe harbors."

In 1998, responding in part to the concerns of ISPs regarding their potential liability for the copyright infringement of their users, Congress enacted a number of narrow "safe harbors" for copyright liability. These safe harbors appear in section 512 of the Copyright Act, which in turn appears in title 17 of the U.S. Code (17 U.S.C. § 512). These safe harbors apply only to "online service providers," and only to the extent that the infringement involves four functions: transitory network transmissions, caching, storage of materials on behalf of users (e.g., web hosting, remote file storage), and the provision of information location tools (e.g., providing links, directories, search engines).

Each of these functions, however, is narrowly defined by the statute (e.g., they don't cover what you'd think) and reflects the state of the art in 1998. Because Congress did not anticipate peer-to-peer file sharing when it enacted the safe harbors, many P2P products may not fit within the four enumerated functions. For example, according to an early ruling by the district court[2] in the *Napster* case, an online service provider cannot use the "transitory network transmission" safe harbor unless the traffic in question passes through its own private network. Many P2P products will, by their very nature, flunk this requirement, just as Napster did.

In addition to being limited to certain narrowly-circumscribed functions, the safe harbors are only available to entities that comply with a number of complex, interlocking statutory requirements:

- The online service provider ("OSP") must (1) adopt, reasonably implement, and notify its users of a policy of terminating the accounts of subscribers who are repeat infringers; and (2) accommodate and not interfere with "standard technical measures" that have been widely adopted on the basis of industry-wide consensus.
- The OSP must designate a "copyright agent" to receive notices of alleged copyright infringement, register the agent with the Copyright Office, and place relevant contact information for the agent on its web site.
- The OSP must, upon receiving a notification of infringement from a copyright owner, expeditiously remove or disable access to the infringing material ("notice and takedown").
- The OSP must not have known about the infringement, or been aware of facts from which such activity was apparent (i.e., if you take a "head in the sand" approach, you lose the safe harbor).
- The OSP must not receive a direct financial benefit from infringing activity, in a situation where the OSP controls such activity.

In the final analysis, qualifying for any of the DMCA safe harbors requires careful advance attention to the legal and technical requirements and obligations that the statute imposes. As a

[2] *See A&M Records v. Napster,* No. C 99-5183 MHP (N.D. Cal. filed May 5, 2000) (available at < http://www.eff.org/IP/P2P/Napster/DMCA_Ruling.php>)

result, any P2P developer who intends to rely on them should seek competent legal counsel at an early stage of the development process—an after-the-fact, "bolt on" effort to comply is likely to fail (as it did for Napster).

D. The DMCA ban on circumvention technologies.

One recent addition to the copyright landscape deserves special attention. Section 1201 of the Copyright Act, enacted as part of the Digital Millennium Copyright Act ("DMCA"), makes it unlawful to "circumvent" any technology aimed at protecting a copyrighted work. In addition, the development, distribution or use of circumvention technology or devices is, with only narrow exceptions, also unlawful. For example, if a copyright owner uses a digital rights management ("DRM") solution to protect a song, it would be unlawful for anyone to crack the encrypted file without the copyright owner's permission, or to build or distribute a software tool designed to crack the file.

Of course, circumvention technology is not a necessary part of a P2P file-sharing network. Today's P2P protocols, such as Bit Torrent, FastTrack and gnutella, simply facilitate file transfers, leaving the file itself, whether encrypted or not, unaltered. Nevertheless, as copyright owners begin to deploy DRM and watermarking systems, there may be interest in integrating circumvention tools with file-sharing tools. In particular, any "spoofing" of authentication handshakes between applications can create concerns (*see, e.g., Real Networks v. Streambox,* 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. Jan. 18, 2000)).

VI. Lessons and guidelines for P2P developers.

A few general guidelines for P2P developers can be derived from the discussion above. These are steps you can take that may: (1) reduce the chance that your project will be an easy, inviting target for copyright owners; and (2) minimize the chances that your case will become the next legal precedent that content owners can use to threaten future innovators.

Of course, because the relevant legal principles are still in flux, these guidelines represent merely one, general analysis of the legal landscape. Please consult with an attorney regarding your precise plans.

1. Do not make or store copies.

This one may be obvious, but remember that if you make or distribute any infringing copies (even if only in RAM) of copyrighted works, you may be held liable as a direct infringer. In that case, a plaintiff need not prove "affirmative acts" or "intent" or "control" or "knowledge" or "financial benefit" or "material contribution"—the fact that copies were made on your equipment can be enough to establish direct infringement liability, whether you knew about them or not.

Of course, this shouldn't be a problem for most P2P developers, since the great insight of peer-to-peer architectures is that the actual resources being shared need not pass through any central server. Nevertheless, be careful where caching or similar activities are concerned.

2. Do not promote, encourage, or foster infringing uses.

In the wake of the Supreme Court's ruling in *MGM v. Grokster*, developers will want to give a wide berth to any conduct that can be viewed as inducing infringing uses of any file sharing application.

Inducement liability turns on the combination of "affirmative acts" and "intent" to encourage or foster infringing activity. Unfortunately, it can be very difficult to prove what your "intent" was—intent is often proved by circumstantial evidence, which means that every email (internal and external), customer support message, conversation (internal and external), and scrap of marketing material might be deemed relevant by a court. In other words, there may be little you can do to definitively resolve the "intent" question.

Fortunately, you have a better chance of controlling whether you engage in any "affirmative acts" that encourage infringement. Accordingly, it is imperative that P2P developers avoid anything that could be construed as an "affirmative act." The following may be worth scrutinizing closely:

- Marketing and promotional materials (including websites, advertisements, press releases, newsletters, or links to third party reviews or testimonials); and
- Any instructions aimed at users (including screenshots, FAQs, and customer support communications, whether in email, chat, or bulletin board postings).

Recall, as well, that the Supreme Court found that an effort to attract users who are known to be copyright infringers (like users of the former Napster software) could constitute an "affirmative act" aimed at fostering infringement.

Finally, it is unclear when you might be held responsible for the statements of third parties. In *MGM v. Grokster,* the Supreme Court found that sending a newsletter with links to news articles that mentioned infringing uses might be an "affirmative act" for inducement purposes. In light of this, special caution is warranted if you disseminate, host, or otherwise adopt statements of third parties who talk about infringing uses. So, for example, you may want to exercise special caution if you host a bulletin board or other forum where users talk directly to each other about infringing uses of your software.

3. Your two options: total control or no control.

In the wake of recent decisions on indirect copyright liability, it appears that copyright law has foisted a binary choice on P2P developers: either build a system that allows for thorough monitoring and control over end-user activities, or build one that makes such monitoring and control impossible.

Contributory infringement arises when you have "knowledge" of, and "materially contribute" to, someone else's infringing activity. The chief battleground for contributory infringement in the P2P cases so far has been the "knowledge" issue, with copyright owners dumping box-loads of infringement notices on software developers, hoping to create "knowledge" of the infringing activities of end-users.[3]

The law of contributory infringement therefore presents a developer with a binary choice: you can either include mechanisms that enable monitoring and control of user activities (and use

[3] As noted in footnote 1, it is not clear whether the new inducement theory announced by the Supreme Court in *MGM v. Grokster* has replaced the traditional contributory infringement analysis. Inducement focuses on a defendant's intent, while traditional contributory infringement focused on a defendant's knowledge. Until this issue is clarified, P2P developers should take care to avoid actions that would give rise to liability under either approach.

them to stop allegedly infringing activity when you receive complaints), or choose a truly decentralized architecture wherein such monitoring and control is impossible without extensive redesign. (Copyright owners have begun arguing that you must redesign future versions of your software to prevent infringement. This argument has never been accepted, but the Supreme Court did say that a failure to take steps to implement filtering can be relevant to establishing "intent" for inducement purposes.)

Vicarious liability also requires that the plaintiff demonstrate that you "control," and receive "benefit" from, someone else's infringing activity. The "benefit" element will be difficult to resist in many P2P cases (at least for commercial products)—so long as the software permits or enables the sharing of infringing materials, this will serve as a "draw" for users, which may be enough "benefit" to result in liability according to some precedents.

So the fight will likely center on the "control" element. The *Napster* court found that the right to block a user's access to the service was enough to constitute "control." The court also found that Napster had a duty to monitor the activities of its users "to the fullest extent" possible. Accordingly, in order to avoid vicarious liability, a P2P developer would be wise to choose an architecture that makes control over end-user activities impossible.

On this front, open source software developers may have an advantage over those who distribute only proprietary object code, insofar as an open source developer can credibly argue that it has virtually no ability to control, or even redesign, its software once distributed. After all, if a developer were to add "filtering" or other restrictions to its software, end-users could simply delete those restrictions and recompile the source code themselves.

4. Better to sell stand-alone software products than on-going services.

Vicarious liability is perhaps the most serious risk facing P2P developers. Copyright owners will argue that having the power to terminate or block users from accessing the network is enough "control" to justify imposing vicarious liability. Add "financial benefit" in the form of a business model that depends on a large user base, and you're well on your way to being held vicariously liable. This is true even if you are completely unaware of what your users are up to—the pairing of "control" and "financial benefit" can be enough.

Of course, most "service" business models fit this "control" and "benefit" paradigm. What this means is that, after the *Napster* decision, if you offer a service, you may have to monitor and police your users if you want to escape liability. If you want to avoid monitoring obligations, you'll have to give up on anything that smacks of "control."

As a result, vendors of stand-alone software products may be in a better position to resist monitoring obligations and vicarious liability. After Sony sells a VCR, it has no control over what the end-user does with it. Neither do the makers of photocopiers, optical scanners, or audio cassette recorders. Having built a device with many uses, only some of which may infringe copyrights, the typical electronics manufacturer has no way to "terminate" end-users or "block" their ability to use the device. They also have no ability to repossess or remotely modify the device after purchase. The key here is to let go of any control you may have over your users—including remote kill switches, automatic update features, contractual termination rights, or other similar mechanisms.

5. What are your substantial noninfringing uses?

If your product is intended to work solely (or best) as a mechanism for copyright piracy, you're asking for legal trouble. More importantly, you're thinking too small. Almost all peer-to-peer systems can be used for many different purposes, some of which the creators themselves fail to appreciate.

So create a platform that lends itself to many uses. Actively, sincerely, and enthusiastically promote the noninfringing uses of your product. Gather testimonials from noninfringing users. The existence of real, substantial noninfringing uses will increase the chances that you can invoke the *Betamax* defense if challenged in court.

6. Disaggregate functions.

Separate different functions and concentrate your efforts on a discrete area. In order to be successful, peer-to-peer networks will require products to address numerous functional needs—search, bootstrapping, namespace management, security, dynamic file redistribution, and user support, to take a few examples. There's no reason why one entity should try to do all of these things. In fact, the creation of an open set of protocols or APIs, combined with a competitive mix of interoperable, but distinct, applications is probably a good idea from a product-engineering point of view.

This approach may also have legal advantages. If Sony had not only manufactured VCRs, but also sold all the blank video tape, distributed all the TV Guides, and sponsored clubs and swap meets for VCR users, the *Betamax* case might have turned out differently. Part of Napster's downfall was its combination of indexing, searching, and file sharing in a single piece of software. If each activity is handled by a different product and vendor, on the other hand, each entity may have a better legal defense to a charge of infringement.

A disaggregated model, moreover, may limit what a court can order you to do to stop infringing activity by your users. As the *Napster* court recognized, you can only be ordered to police your own "premises"—the smaller it is, the less you can be required to do.

In addition, certain functions may be entitled to special protections under the "safe harbor" provisions of the DMCA. Search engines, for example, enjoy special DMCA protections. Thus, the combination of a P2P file sharing application with a third party search engine might be easier to defend in court than Napster's integrated solution.

Finally, in the wake of the *MGM v. Grokster* ruling, copyright owners may argue that certain features, if implemented as part of a file-sharing application, constitute evidence of inducement. They have already singled out features intended to provide anonymity (e.g., proxies) and network integrity (e.g., IP blocklists, anti-spoofing features) for criticism. While no court has yet ruled that a product feature can, by itself, support an inducement claim, it may be wise to leave those features to third parties and leave it to your users to figure out how to use them. Incorporating simple APIs (like support for SOCKS proxies and user-configurable IP blocklists) can make this easier and stimulate interoperability among different network services.

7. Don't make your money from the infringing activities of your users.

Avoid business models that rely on revenue streams that can be directly traced to infringing activities. For example, a P2P file-sharing system that includes a payment mechanism

might pose problems, if the system vendor takes a percentage cut of all payments, including payments generated from sales of bootleg Divx movie files.

8. Give up the EULA.

Although end-user license agreements ("EULAs") are ubiquitous in the software world, copyright owners have attempted to use them in P2P cases to establish "control" for vicarious liability purposes. On this view, EULAs represent "contracts" between vendors and their users, and thus give software vendors legal control over end-user activities. EULAs that permit a vendor to terminate at any time for any reason may raise particular concerns, insofar as they may leave the impression that a vendor has the legal right to stop users from using the software.

P2P software vendors should consider distributing their code without a EULA. Even without a EULA, a software developer retains all of the protections of copyright law to prevent unauthorized duplication and modifications. (After all, books, DVDs, and music CDs are all sold without any EULA, and copyright law certainly protects them.)

9. Beware direct customer support.

Any evidence that you have knowingly assisted an end-user in committing copyright infringement will be used against you. In the P2P cases so far, one source for this kind of evidence is from customer support channels, whether message board traffic, instant messages or email. A user writes in, explaining that the software acted strangely when he tried to download *The Matrix*. If you answer him, copyright owners will make it seem that you directly assisted the user in infringement, potentially complicating your inducement or contributory infringement defenses.

Fortunately, user communities often can and do support themselves in whatever forums they like. As a result, there may be no need for one-on-one customer support from the developers of the software (this will be even more likely if the software is open source and expert users can see how it works for themselves).

10. Be open source.

In addition to the usual litany of arguments favoring the open-source model, the open source approach may offer special advantages in the P2P realm. It may be more difficult for a copyright owner to demonstrate "control" or "financial benefit" with respect to an open source product. After all, anyone can download, modify and compile open source code, and no one has the ability to "terminate," "block access," implement "filtering," or otherwise control the use of the resulting applications. Any control mechanisms (including "filtering"), even if added later, can simply be removed by users who don't like them.

"Financial benefit" may also be a problematic concept where the developers do not directly realize any financial gains from the code (as noted above, however, the *Napster* court has embraced a very broad notion of "financial benefit," so this may not be enough to save you). Finally, by making the most legally dangerous elements of the P2P network open source (or relying on the open source projects of others), you can build your business out of less vulnerable ancillary services (such as search services, bandwidth enhancement, file storage, meta-data services, etc.).

Finally, as mentioned above, expert end-users may be better able to provide customer support for the user community if they can see for themselves how the code works, relieving the

developers of the burden of providing customer support. This may be particularly relevant, as copyright owners have focused on customer support interactions when gathering evidence to use against P2P developers.

* * *

About the Author: Fred von Lohmann is a senior staff attorney with the Electronic Frontier Foundation, specializing in copyright and trademark issues. He represented StreamCast Networks in the *MGM v. Grokster* litigation, one of the leading cases addressing copyright and peer-to-peer file sharing. In addition to litigation, he is involved in EFF's efforts to educate policy-makers regarding the proper balance between intellectual property protection and the public interest in fair use, free expression, and innovation.

[4] Terms available at: <http://creativecommons.org/licenses/by-nd-nc/1.0/>.