STATE BAR OF MICHIGAN

MICHIGAN COMPUTER LAWYER

State Bar of Michigan Computer Law Section www.michbar.org/computerlaw/home.html November/December 2003 Volume 21, No. 2.

Contents

Michigan Computer Lawyer is published bi-monthly. If you have an article you would like considered for publication, send a copy to:

Matthew M. Jakubowski
Brooks Kushman, PC
1000 Town Center
Floor 22, Suite 2200
Southfield, MI 48075-1183
E-Mail: mjakubowski@brookskushman.com

Comments from Outgoing Editor

This last issue of 2003 brings a fresh new look to the Computer Lawyer Newsletter. The cosmetic change is long overdue and it seems apropos that it should coincide with a substantive change. It has been my pleasure to serve as newsletter editor for the past few years, but it is time for me to move on. I am pleased to announce that Matt Jakubowski of Brooks Kushman, PC has agreed to take over as newsletter editor beginning in 2004. I wish the best to Matt in his new role as editor and wish all of the members of the Computer Law Section a happy and prosperous New Year!

-Paul J. Raine

Comments from Incoming Editor

Paul, thank you for the introduction and for your efforts as the newsletter editor over the last couple of years. I look forward to serving as editor for 2004 and striving to meet the high standards established by Paul. As the editor of the newsletter, I invite members of the Computer Law Section to actively participate in preparing articles for consideration in the newsletter. If writing articles is not your cup of tea, I will embrace any ideas that the membership has for improving the newsletter, for example, identifying topics that you want to see in upcoming newsletters. Well, enough for my introduction, it is time for the content of the newsletter to take center stage.

-Matt Jakubowski

Statement of Editorial Policy

The aim and purpose of the Michigan Computer Law Section of the State Bar of Michigan is to provide information relative to the field of computer law, and other information that the section believes to be of professional interest to the section members.

Unless otherwise stated, the views and opinions expressed in the Michigan Computer Lawyer are not necessarily those of the Computer Law Section, or the State Bar of Michigan.

System Failure: Has the A&M v. Napster Decision Been Rendered Obsolete in the War Against Peer-to-Peer File-Sharing Networks?

By: George K. Pitchford (Ed Langs Writing Contest 1st Place Winner)

I. Introduction

To the chagrin of the entertainment industry, currently, a multitude of copyrighted files are available to connected Internet users around the world. Although copyright infringement has plagued the music and movie industry in one form or another since the dawn of the digital revolution, recently the outright theft of their product has reached near epic proportions. Undoubtedly, this latest onslaught is at least partially due to the new phenomenon of peer-to-peer file sharing.

Peer-to-peer networks allow even novice users to easily connect and download files directly from another user's systems. Also, since participating users are able to easily share their own recently downloaded files, the wealth of copyrighted material available on these networks continues to grow exponentially.

Copyright holders throughout the entertainment industry have taken action to quell this free flow of information, and have declared war on peer-to-peer file-sharing networks. The most notable casualty was the now infamous Napster.[1] At its height, Napster boasted over ninety million registered users, and was easily the fastest growing Internet service in the world.[2] However, before the Internet upstart could even begin to make a profit, the entertainment industry led by Record Industry Association of America (RIAA), a trade group representing the five largest record companies, brought a lawsuit and successfully shut down the service.[3]

On January 9, 2003, yet another volley was fired in the war between copyright holders throughout the entertainment industry and peer-to-peer file network operators.[4] Metro-Goldwyn Studios, in conjunction with a myriad of other entertainment companies, successfully argued that a California Federal Court could assert jurisdiction over various companies operating peer-to-peer networks from outside of the United States.[5] Consequently, this consortium of record and movie moguls will be allowed to proceed with its case alleging copyright infringement against some of the biggest peer-to-peer networks currently in existence.[6]

Much like in the *Napster* case[7], the Plaintiffs in *Metro-Goldwyn* are alleging that the targeted peer-to-peer file-sharing services are guilty of contributory and vicarious copyright infringement.[8] If successful, the plaintiffs could essentially hold the targeted peer-to-peer networks such as Grokster or Kazaa liable for countless acts of infringement actually committed by the networks' users. Considering how effective this strategy was against the original peer-to-peer goliath Napster, there definitely seems to be cause for concern amongst the popular peer-to-peer network operators.

This past success notwithstanding, copyright holders relying on the *Napster* decision in future litigation against the current generation of peer-

to-peer file-sharing services might find themselves on the battlefield with no bullets. Not only have peer-to-peer network operators taken practical steps to avoid liability[9], but they have also revamped the architecture of their networks so that they can take an even further step back from the infringing activity of their users. By using this upgraded variation of the original peer-to-peer architecture, network operators have managed to place themselves out of the legal reach of even rulings against peer-to-peer networks, including the *Napster* decision.[10]

This article will examine the law underlying the *Napster* decision, the *Napster* decision itself, and whether, in light of recent innovations, the reasoning emerging from the Napster decision is still even relevant in the ongoing war against current peer-to-peer network operators.

II. Peer-to-Peer Networks

A. What is a Peer-to-Peer Network?

Currently, the Internet's architecture is mainly based on a spoke-and-hub design.[11] This requires users who want to send or receive information to do so through a central system known as the server.[12] Servers, which are usually larger, more powerful systems, serve only as hubs, where Internet traffic is routed either to other hubs or directly to other users connected to that hub.[13] The user's system, on the other hand, serves as a spoke connected to the hub, and is limited to only sending or receiving information through the hub.[14] Thus, all users wishing to send or receive any data are dependent on a centralized hub in one form or another.

Peer-to-peer networking removes these proverbial chains from users. It allows the user's system to serve as both a spoke and a hub.[15] Accordingly, users on a peer-to-peer network are able to simultaneously send and receive information with each other without ever using a third-party hub.[16] Each user's system becomes a server, while still allowing him or her to search out and download information.

Most of the software used to access the bounty of copyrighted files on peer-to-peer networks is similar. Network operators usually offer the required software free to users in order to bolster their user base, thus increasing the number of files that will be available. Some peer-to-peer networks require users to actually sign onto the network with an account, while others allow anonymous access. Once connected, users are able to select which files on their own system to offer for download to others connected to the network, and are able to directly search and download files available on other users' systems.

Ironically, this seemingly unique innovation actually represents a return to the original architecture of the Internet. [17] In its infancy the purpose of the Internet was to serve as an alternative means of communication for the military in case of a nuclear attack. [18] It was essential that the system still be able to operate even if a large portion was disabled.[19] Consequently, designers purposely avoided the more centralized spoke-and-hub design, where the destruction of the more essential hubs could lead to disaster for the entire network.[20] Instead, they designed what was probably the first peer-to-peer network, where users' systems could communicate with one another even in the absence of a centralized hub.[21] It was not until the later commercialization of the Internet that this decentralized architecture was abandoned for the seemingly faster and more efficient spoke-and-hub design of today.[22]

B. Peer-to-Peer Technology and Copyright Infringement

Although dormant for many years, Internet entrepreneurs throughout the world have now realized the potential for the decentralized architecture of peer-to-peer networks. Examples of future applications of peer-to-peer networks are countless. Some commentators foresee peer-to-peer networks revolutionizing how users search the Internet. Theoretically, peer-to-peer networks could provide real time searches of sites actually on the Internet, as opposed to current engines that search through cached catalogues that sometimes produce outdated and erroneous results.[23]

Unfortunately for various copyright holders throughout the entertainment industry, however, most users have embraced the anonymity, convenience, and freedom of peer-to-peer networks as a means of acquiring and disseminating countless gigabytes of copyrighted files. Adding to the problem is the fact that unlike their predecessors such as Napster, current peer-to-peer networks are able to not only offer music files, but also movies, software, and even published materials such as best-selling novels.

Considering that some of the more popular peer-to-peer networks may have as many as four million users simultaneously signed on, the wealth of files available is incredible. Currently, no official studies exist on what proportion of the files available on most peer-to-peer networks are protected by a copyright. However, as much as eighty-five percent of the files on peer-to-peer predecessors, such as Napster, were estimated as being offered in violation of a copyright.[24] Essentially, peer-to-peer networks have been transformed into a lawless frontier, where copyrights are openly disregarded, and files containing popular music, movies and software are easily downloaded by millions of users on a daily basis.

C. Peer-to-Peer Networks: The Old vs. The New

Currently, peer-to-peer networks can basically be categorized as either centralized or decentralized. Although, as earlier mentioned, the major goal behind peer-to-peer networks is to establish a decentralized network, first generation services, such as Napster, were not entirely devoid of centralized servers.[25] Early peer-to-peer networks, including Napster, used centralized servers to maintain a network "search index".[26] The search index contained the name and location of every file available for download on every user's system connected to the network. Thus, when a user would search for a file on the network, he or she would actually be probing through the search index on the central server, which would then return matching results back to the user.[27] Although no files were ever actually exchanged over the central server, by indexing and locating the desired file for the user, these peer-to-peer networks essentially acted as brokers in the file sharing process.

Decentralized peer-to-peer networks, however, take an even further step back from the file transfer process. By utilizing specialized software, such as Fast-Track, current peer-to-peer networks have been able to dispense with centralized servers entirely.[28] Observers of this next generation of peer-to-peer networks have noted that decentralized peer-to-peer networks are "not run from a central location like Napster[,] [i]nstead [they] exis[t] as an amalgamation of individual users that connect to each other via the internet to share audio files with the fast-track software."[29] Consequently, unlike their centralized predecessors, decentralized peer-to-peer networks truly have no ability to monitor what their network is being used for.[30]

III. The Applicable Law

Considering the decentralized nature of peer-to-peer networks, it would be almost impossible to hold them liable for direct infringement. All file transfers occur directly between users, with little or no participation by the operators. This fact notwithstanding, legitimate copyright holders are not powerless against defendants who do not directly participate in the infringement. Copyright law offers at least two claims, namely contributory and vicarious copyright infringement, that allows a third party to incur liability in spite of the fact they may not have directly participated in the infringement.

A. Contributory Copyright Infringement

Contributory copyright infringement "stems from the legal notion that one who directly contributes to another's infringement should be held accountable."[31] Although the U.S. Copyright Act[32] does not have a specific provision for a claim of contributory infringement, the U.S. Supreme Court has made it clear that it is not precluded from being applied in its common law form.[33] Much of the common law forming contributory copyright infringement is based on enterprise liability, and "imposes liability where one person knowingly contributes to the infringing conduct of another."[34] In order to establish liability based on contributory infringement it must be proven that the defendant had "knowledge, constructive or actual, of the infringing activities of others and materially contribut[ed] to the infringing actions."[35]

Although at first glance this definition seems somewhat self-explanatory, courts have struggled with what exactly is a "material contribution" and what level of "knowledge" is necessary in order to incur contributory infringement liability.

Each of these issues was resolved to some degree in *Fonovisa v. Cherry Auction*, one of the seminal cases on contributory copyright infringement.[36] In *Fonovisa*, copyright owners alleged that the operators of a large swap meet were guilty of contributory copyright infringement stemming from the meet operators allowing the sale of pirated copies of copyrighted albums by independent swap meet vendors.[37] Copyright holders claimed that the swap meet operators either knew or should have known of the copyright infringement being committed by vendors and were

therefore liable for contributory copyright infringement.

The Court upheld the copyright owners' claim of contributory infringement, and held that "contributory liability is applicable if the defendant (1) intentionally induces another to infringe on a trademark or (2) continues to supply a product knowing that the recipient is using the product to engage in trademark infringement."[38] Furthermore, the court addressed the issue of materiality by concluding that the infringing activity could not have easily taken place without the services and venue provided by the Defendant, thus the Defendant's actions or inactions constituted a material contribution.[39]

Fonovisa seems fairly damning for any third party, including peer-to-peer network operators, who knowingly provides any product that may be used for the purpose of infringement. However, cases subsequent to *Fonovisa* should also be considered, especially those involving online providers and decided within the context of the digital revolution. For instance, in *Religious Technology Center v. Netcom On-Line Communication* a Federal District Court recognized that because of the nature of the Internet, service providers could not be held to the rigid standard of liability for contributory copyright infringement as in *Fonovisa*.[40] The Court went on to hold that for a service provider utilizing the Internet, such as peer-to-peer networks, to be held liable for contributory infringement, there must be evidence that they had actual knowledge of the underlying infringement by users. [41]

It should be noted that this latest development in copyright law does not allow online defendants to take a posture of willful blindness in order to avoid claims of contributory copyright infringement.[42] In fact, if a copyright holder is able to catalog and present evidence to a service provider of how and where their system is being used for copyright infringement, that operator has a duty to purge their system of the identified copyrighted materials.[43]

Thus, case law would seem to indicate that in order to maintain a claim of contributory copyright infringement against a network operator, a plaintiff must allege more then just the fact that the disputed technology may be used for infringing purposes. Additionally, evidence must be presented to support the inference that the service provider had *actual* knowledge of its users infringing activity.[44]

B. Vicarious Copyright Infringement

Contributory copyright infringement is not the only claim available to copyright holders against operators not directly involved in infringement. Courts have also recognized the claim of vicarious copyright infringement, which allows for recovery against defendants who have profited from the direct infringing activity of individuals they have control over.

Vicarious copyright infringement is based on the principles of agency law, and the tort concept of respondent superior.[45] Traditionally, under the concepts of agency and respondent superior, courts have allowed plaintiffs to hold employers responsible for the actions of their employees while performing work duties.[46] When reviewing claims of vicarious copyright infringement, courts have done away with the requirement of an employee-employer relationship and now concentrate on (1) the defendant's ability to control the direct infringement activity and (2) the financial interest that the defendant may have in the direct infringement.[47] In other words, the purpose of vicarious copyright infringement is to impose liability on those who directly profited from the infringement of a third party, which they had the power to prevent.

The United States Court of Appeals further developed the concept of vicarious copyright infringement in the landmark case of *Shapiro v. H.L. Green*.[48] In *Shapiro*, a storeowner had directly profited from the sale of bootlegged records within his own store by a third-party vendor.[49] Although the defendant received a portion of the gross sales of the bootlegged records from the in-store vendor and retained the right of supervision over the vendor, the storeowner never directly took part in the infringing conduct.[50] This fact notwithstanding, the plaintiff sought to hold the storeowner vicariously liable for not only allowing the infringing conduct to continue, but also for profiting from it. The defendant, for its part, continued to assert that it simply licensed the vendor to conduct business within its store, and should not be held liable for whatever egregious acts were committed by the licensee.

In coming to its decisions, the Court in *Shapiro* closely reviewed two lines of cases. First, the court examined cases where landlords had leased property to tenants, who in turn used the rental property in schemes involving copyright infringement.[51] These cases hold that "[where a] landlord lets his premises without knowledge of the impending infringement by

his tenant, exercises no supervision over him, charges a fixed rental and receives no other benefit from the infringement, and contributes in no way to it . . . the landlord is not liable for his tenant's wrongdoing."[52] The court went on to contrast this line of cases to those involving managers or owners of a music halls who "leas[e] [their] premises to or hir[es] a band, which bring[s] in customers and profits to the proprietor by performing copyrighted music but without complying with the terms of the Copyright Act."[53] In these cases the managers and owners "[were held] liable for the infringement of copyright resulting from the performance of a musical composition by a band or orchestra whose activities provide the proprietor with a source of customers and enhanced income."[54] Furthermore, the court also held a proprietor or manager's ignorance of a moneymaking performer's infringement would not immunize him from liability.[55]

The Court in *Shapiro* went on to hold that the defendants' actions were more analogous to the music hall owner, and held them vicariously liable for the copyright infringement committed by the vendor.[56] Essentially, the Court concluded that because the storeowner had control over the licensee, and also profited from the infringement in the form of commissions and profit sharing, he should also have to share in the vendor's direct liability for copyright infringement.[57]

After *Shapiro* and its progeny, it became clear that when reviewing claims of vicarious copyright infringement the court would look at the defendant's actual control over the direct infringer, and also, whether the defendant derived any direct financial benefit from the infringement.[58]

C. Summary of the Law

Obviously, the above is far from an exhaustive list of possible claims that could be brought against the current generation of peer-to-peer networks. However, based on the strategy employed by copyright holders in the *Napster* case, they are most likely the tactics that will be relied upon. Even in *Metro-Goldwyn*, one of the entertainment industries' latest attacks on peer-to-peer networks, it would appear a large part of their claim rests on theories of contributory and vicarious copyright infringement.[59]

It should be noted that just because these tactics were successful against other peer-to-peer networks, most notably Napster, it does not guarantee success against the newer networks. As mentioned above, most current peer-to-peer networks have taken a host of precautions, both practical and technological, in an attempt to protect themselves from liability. Furthermore, as will be discussed below, certain legal defenses may be successfully asserted by the current targeted defendants, which may put them beyond the scope of either of these claims.

IV. Defenses

Peer-to-peer networks are not entirely defenseless against claims of infringement that may or have been brought by the entertainment industry. Admittedly, some of the more traditional defenses such as fair use will probably not be available to peer-to-peer networks.[60] Network operators, however, may still be able to rely on both statutory and judicially recognized defenses to fend off future attacks. Although the defenses discussed below were unsuccessfully asserted in the Napster case, recent innovations and technical differences between Napster and current peer-to-peer networks may lead to different and more favorable outcomes for peer-to-peer networks.

A. Substantial Non-Infringing Use Doctrine

As mentioned above, lawmakers and courts alike have long recognized that limits are necessary on the exclusivity rights of a copyright holder. Accordingly, claims of contributory infringement based on the fact that a defendant's product may be used for infringing purposes have been rejected by courts.[61] In fact, under the Substantial Non-Infringing Use Doctrine (hereinafter Substantial Use), in order to avoid liability a Defendant need only show that its product is "capable of substantial noninfringing uses."[62] Thus, even where a product may be used to infringe upon a copyright, if the defendant can prove that other substantial and noninfringing uses exist then it would be possible to avoid contributory infringement liability.[63]

The leading case developing the Substantial Use Doctrine is *Sony v. Universal Studios*. This case is important to the discussion of peer-to-peer networks, because it directly addresses the proposition that a defendant should be held liable merely for selling a product that may be used for copyright infringement.[64] However, what is also important to note is the almost

eerie parallels between how the entertainment industry copyright holders reacted to the introduction of new technology then, and how they currently have chosen to react to the new technology and capabilities of peer-to-peer networks.

In the early 1980's Sony introduced new technology that allowed consumers to tape and then later view television shows.[65] This technology known as the VTR, now more commonly known as the VCR, quickly began showing up in households all over America. Afraid for the integrity of their copyrights, television producers rushed to suppress the new technology.[66] In 1983, they brought suit against Sony claiming that the electronics corporation was liable for contributory and vicarious copyright infringement because they had provided technology to consumers with the ability to infringe upon copyrights.[67] After exhausting all remedies and solutions offered by lower courts, the dispute was finally brought before the U.S. Supreme Court to be settled.

In *Sony*, the Court recognized that there was no precedent within U.S. copyright law for finding a defendant guilty of contributory infringement for simply selling an item that could be used for infringing purposes.[68] Consequently, the Court turned to copyright law's legal sibling patent law for guidance on the issue.[69] After a careful review of applicable patent cases considering the limits of a claim of contributory infringement, the Court held that "[the] sale of an article which though adopted to an infringing use is also adapted to other and lawful uses, is not enough to make the seller a contributory infringer. Such a rule would block the wheels of commerce."[70]

In short, *Sony* seems to provide defendants facing claims of contributory infringement with a defense by importing the Substantial Use Doctrine into copyright law from patent law. Accordingly, if a defendant is able to show that alternative, non-infringing applications exist for a potentially infringing technology, operators cannot be held liable.

With the seemingly endless actual and potential non-infringing uses of peer-to-peer networks, the Substantial Use defense could play a vital role in the future of peer-to-peer networks. However, as pointed out by the Federal District Court in the *Napster* case, peer-to-peer network operators must pay close attention to the limits of the Substantial Use defense and the *Sony* decision.[71] In spite of this warning, the Substantial Use Doctrine could be valuable to any peer-to-peer defendant targeted by the entertainment industry with claims of contributory copyright infringement.

B. Digital Millennium Copyright Act – The Safe Harbor

In November 1998, Congress enacted the Digital Millennium Copyright Act (hereinafter the "DMCA") as Chapter 12 of the Copyright Act.[72] Despite the DMCA's seemingly pro-copyright holder slant[73], within the legislation a limited protection from copyright infringement liability was provided to online service providers.[74] This provision within the DMCA limiting infringement liability is known as the "safe harbor" provision. Presumably, the purpose of the safe harbor provision is to ensure that copyright law and the protections it offers do not directly or indirectly stifle the growth and innovation necessary for technology such as the Internet to continue to grow. This grant of limited immunity by Congress could serve as a refuge for future peer-to-peer network operators facing claims of contributory or vicarious copyright infringement.

Section 512(a), the safe harbor provision, of the DMCA extends this immunity only if five conditions are met.[75] Specifically, service providers must show that

> (1) the transmission of the material was initiated by or at the direction of a person other then the service provider;
> (2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;
> (3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;
> (4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonable necessary for the transmission, routing, or provision of connections; and
> (5)the material is transmitted through the system or network without modification of its content."[76]

Together, these factors lay the groundwork for what is necessary to qualify for immunity from copyright infringement under the DMCA.

Arguably peer-to-peer networks fulfill all five of the requirements necessary to obtain immunity from copyright liability under the DMCA. The decentralized nature of peer-to-peer networks puts users in complete control to initiate the sending or receiving of files. Also, due to the architecture of peer-to-peer networks, it is not necessary for operators to store any of the transferred files on their network, and this direct connection also ensures that files are not in any way modified by the network operator.

In spite of fulfilling all five requirements under section 512(a) of the DMCA, it remains unclear if peer-to-peer networks would receive protection under the provision.[77] As courts and commentators alike have noted, this section only provides protection to service providers, and it has not been fully resolved as to who exactly qualifies as a service provider.

The DMCA does offer some guidance on this issue by expressly providing a definition of a service provider as "an entity offering the transmission, rousting, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the materials sent or received."[78] Ironically, because of the decentralized nature of peer-to-peer networks and how transferred files never actually flow through centralized servers, the very feature that may protect them from other forms of infringement liability, some commentators have argued that peer-to-peer networks operators should not fall under this rather esoteric definition of service provider.[79]

The Courts themselves even seem somewhat confused as to who qualifies as a service provider under the safe harbor provision of the DMCA. One of the many rulings to emerge from the Napster dispute concluded that peer-to-peer networks did not qualify as service providers.[80] Relying largely on legislative history the Court concluded that Napster failed to fall under the protection of the safe harbor because "it does not transmit, route, or provide connections for allegedly infringing material through its system."[81] However, other courts considering the eligibility of peer-to-peer networks have come to the exact opposite result. In fact, another Federal District court considering the eligibility of Aimster, a peer-to-peer network operator similar to Napster, concluded that "[a] plain reading . . . reveals that 'service provider' is defined so broadly that we have trouble imagining the existence of an online service that would not fall under the defintio[n.]"[82] The Court went on to hold that Aimster, a peer-to-peer network, *did* qualify under the safe harbor's definition of service provider.

Despite the seeming confusion over whether peer-to-peer networks are protected under the safe harbor provisions of the DMCA, at the very least a viable argument exists that peer-to-peer networks are immune from copyright liability as service providers. What remains to be resolved is whether courts will interpret the provision's definition of service provider to include peer-to-peer networks.

C. Summary of Defenses

Peer-to-peer networks facing claims of contributory or vicarious infringement are far from defenseless. Although the source of some frustration, the relative novelty of peer-to-peer networking has left it unclear as to how successful these may be in future litigation. In spite of groundbreaking precedents such as *Napster*, it is still unclear how courts will interpret and apply these defenses to peer-to-peer networks. This leaves future targets of the entertainment industry having to speculate and prepare for almost anything.

V. The Napster Case – End Game?

Admittedly, the law regarding the liability surrounding peer-to-peer networks operators is somewhat unclear. The *Napster* case, however, probably represents the courts best attempts to date to settle some of the issues regarding peer-to-peer networks.[83] *Napster* also serves as an example of how courts in the digital age have often been forced to apply legal doctrines and concepts to new technologies that have the potential to revolutionize the Internet.

Presumably, the Court's purpose in the *Napster* case was to try and define boundaries for both copyright holders and peer-to-peer network operators. It is still unclear if this was accomplished. That notwithstanding, what was accomplished was the shutdown of the largest peer-to-peer networks, and a precedent with the potential to restrict the future growth of the peer-to-peer networking concept.

A. The Background of Napster

The Napster program was originally the dream of college freshmen Shawn Fanning.[84] He, along with two friends[85], became obsessed with the idea of creating an application that allowed them to easily upload and download music files from one another.[86] Fanning became so enthralled with developing the application that he dropped out of Northeastern University, and began working on it for countless hours in the backroom of his uncle's computer gaming company.[87] After finishing the application, Fanning decided to dub the fruits of his labor Napster, after his own childhood nickname.[88]

Ironically, Napster was an incredibly simple program. Based heavily on the then forgotten peer-to-peer architecture, Fanning created an application that dispensed with the need of centralized servers, except for the cataloging and location of files. Users would basically be downloading from one another, and Fanning's servers would act as their search engine and gopher.

Fanning instantly recognized the potential for his new application and immediately sought out investors.[89] After forming a corporation, Fanning introduced Napster to the world and literally changed the future of the Internet.[90]

From its inception Napster was a huge success. Users all over the world jumped at the opportunity to be able to freely exchange music files with one another. The music industry, on the other hand, was both enraged and terrified of the idea of Napster. An image began to emerge of the future where their precious and profitable distribution networks were obsolete and no longer needed. Also, they saw this alternative means of obtaining their copyrighted product for free as eventually siphoning off their profits and hastening their impending demise.

With Napster poised to shift from its entirely free service, to their profit-making model[91], concerned record companies finally demanded that the Internet upstart take steps to prevent copyrighted files from being exchanged through its network. Napster refused and the record companies filed suit, and sought a preliminary injunction halting the Napster service during litigation.[92] With potentially billions of dollars and maybe the future of the record industry at stake, the stage was set for one of the first legal battles involving peer-to-peer networks and the potential infringement liability of their operators.

B. The Plaintiff's Claims in Napster

In *Napster*, the plaintiffs claimed that the Defendant was indirectly liable for the copyright infringement of their users.[93] Relying mainly on claims of contributory and vicarious infringement, the Plaintiffs were seeking to either shut down Napster or have their copyrighted files removed from the peer-to-peer network.

Although the separate claims of contributory and vicarious liability were examined above, the *Napster* case supposedly brought the doctrines into the twenty-first century. Furthermore cases such as *Metro-Goldwyn* indicate that the entertainment industry plans on relying heavily on the Napster courts' interpretation of the two claims in future legal battles against peer-to-peer networks. Therefore, how the court in Napster treated the Plaintiffs' claims of contributory and vicarious infringement becomes very important to any discussion about the future of peer-to-peer networking.

1. *Napster's Liability for Contributory Copyright Infringement*

In reviewing the plaintiff's contributory infringement claim, the Ninth Circuit Court of Appeals relied on a traditional definition of how contributory liability is established and quoted the landmark case of *Gershwin*, which stated that "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.'"[94] From this definition the Court felt it necessary to focus on two issues, the extent of Napster's knowledge of its users' infringement and the materiality of Napster's contribution.

Surprisingly, Napster's knowledge of its users' infringement was not constructively established by the nature of its peer-to-peer network. In fact, the Court of Appeals explicitly overturned the lower Court's holding that the requisite knowledge for contributory infringement should be imputed to Napster, simply because they were aware that their peer-to-peer network could possibly be used for infringement purposes.[95] In actuality, what proved that Napster did have knowledge of the infringing activity was an array of internal documents where Napster executives admitted that they knew their service was mainly being used for infringement purposes. Also, prior to litigation, the

plaintiffs had given Napster actual notice of users who were offering files in violation of a copyright. For these reasons, the Court concluded that Plaintiffs would probably establish the element of knowledge necessary to maintain a claim of contributory copyright infringement.

The materiality of Napster's contribution to its users' infringement was much easier for the Court of Appeals to determine. Relying on *Fonovisa*, the Court reasoned that by supplying the site and facilities where the infringement occurred, it would be impossible to conclude that Napster only accidentally took part in the infringing activity. Thus, the Court concluded, the Plaintiffs would probably be able to prove the element of materiality.[96]

2. Napster's Liability for Vicarious Copyright Infringement

The Ninth Circuit Court of Appeals also found that Napster was probably guilty of vicarious copyright infringement. In doing so the court once again relied heavily on the landmark case *Gershwin* and its interpretation of how a defendant may incur vicarious liability. Accordingly, the Court reviewed whether Napster "ha[d] the right and the ability to supervise the infringing activity and also has a direct financial interest in such activities."[97] Thus, the Court turned its attention to the possibility of whether Napster's architecture would allow its operators to supervise or prevent the infringing activity taking place on its network. Also, the Court reviewed what, if any, economic benefit Napster might receive as a result of the infringing activity.

The Court held that Napster did have the requisite supervision of its users infringing activity to incur liability for vicarious copyright infringement.[98] Napster's own use policies indicated that they had the ability to restrict access of specific users.[99] This ability to police its network created a duty to do so.[100] This meant that Napster had "the right and ability to police its system and failed to exercise that right to prevent the exchange of copyrighted material."[101] It is important to note, however, that in recognizing this duty, the Court of Appeals partially reversed the lower court's broader ruling, and expressed important limits. The Court held that this duty to police is not absolute and should be shaped by what the architecture of the defendant's system allows them to accomplish.[102] Accordingly, the Court still found Napster under a duty to police their network, however, this was mainly based on the fact that Napster's centralized architecture and search indices gave its operators the ability to easily track the existence and location of copyrighted files.[103]

Napster's financial benefit from its users was fairly apparent. Case law makes it clear that the financial benefit does not have to flow directly from the infringing activity. As the Court in *Napster* observed, "[f]inancial benefit exists where the availability of infringing material acts as a draw for customers."[104] It is clear that Napster's goal was to increase its user base and then switch to a profit making model based on revenue generating activities such as pop-up advertisements and targeted emails.[105] Therefore, since there was a direct correlation between the amount of copyrighted files offered and the expansion of Napster's user base, the Court held they were deriving financial benefit from the infringing activity.[106]

C. Final Reflections on the Napster Decision

At first, it would seem that the Napster case could serve as a blueprint for handling future peer-to-peer networks whose users take part in copyright infringement. The Plaintiffs were able to secure a preliminary injunction based on the probable success of their claims of contributory and vicarious copyright infringement and shutdown Napster without ever really litigating the facts.

In spite of all of this, it would seem that this victory may turnout to be hollow and bittersweet. Already, questions are beginning to arise about whether this legal strategy will be flexible enough to react to the world technology that changes on an almost daily basis.

VI. Is the Napster Decision Obsolete?

The Court's decision in *Napster* obviously represents a victory for the entertainment industry in its efforts to remove copyrighted material from peer-to-peer networks, or to shut them down entirely. However, what remains to be seen is how permanent is this victory? A close reading of the Court of Appeal's decision reveals that the Court either purposely or inadvertently left numerous holes that may allow future targeted peer-to-peer network operators to slip through the entertainment industries' dragnet.

These gaps within the Ninth Circuit Court of Appeal's reasoning begs the question: Is the *Napster* decision already obsolete? One has to wonder how applicable will the already hazy decision be to the new

generation of peer-to-peer networks that are completely decentralized? It is possible that entertainment industry copyright holders may be in for an unpleasant surprise if they continue to rely on the Napster decision in their ongoing conflict with peer-to-peer network operators.

A. Potential Contributory Copyright Infringement Claims

In *Napster*, the Court made it clear that two elements are necessary to maintain a claim of contributory negligence: knowledge and materiality. Plaintiffs were able to establish knowledge on the part of Napster only based on preexisting extrinsic evidence.[107] In fact, the Court expressly refused to find that Napster had constructive knowledge of the infringement simply because their network could be used for infringement purposes.[108]

This requirement for actual knowledge of the infringing activity could put an enormous burden on copyright holders targeting peer-to-peer network operators. They would be forced to continually monitor these networks, and report offenders to the operators. However, because users are constantly signing on and off of the network, chances are the offending files would be gone or located elsewhere before a copyright holder could even compile a list.

Also, it would seem that the Court of Appeals in *Napster* has practically invited peer-to-peer network operators to assert the substantial use defense to claims of contributory copyright infringement. Although Napster tried to utilize this defense and failed, that may have been due to its centralized peer-to-peer architecture. With centralized peer-to-peer networks operators have knowledge of what files are available for transfer because every file offered is tracked within their search index located on their own servers. Therefore, it could be successfully argued that these operators have actual knowledge of the infringing activity taking place on their network.

Decentralized peer-to-peer networks, however, such as Kazaa or Gnutella, simply do not have this ability. Through a variety of techniques, they allow users to search each other's systems without the aid of a central server. Newer peer-to-peer networks truly have no knowledge of what files are available on their system. Even the Court in *Napster* stated: "absent any specific information which identifies infringing activity, a computer system operator cannot be liable for contributory infringement merely because the structure of the system allows for the exchange of copyrighted material."[109]

Essentially, by eliminating centralized servers, new peer-to-peer network operators have become more like the VTR distributors in the *Sony* case. Thus, in light of the obvious substantial non-infringing uses of the peer-to-peer networks, they may be able to successfully assert the defense to claims of contributory copyright infringement, and avoid liability for the infringing activities of their users.

B. Potential Claims of Vicarious Copyright Infringement

When reviewing the Plaintiffs' claim of vicarious copyright infringement in *Napster*, the court paid special attention to the amount of control the defendants had over their peer-to-peer network.[110] Especially important was whether the operators had the ability to police the exchange of files, and restrict a user's access.[111] Due to the centralized structure of Napster and its search indices, which basically allowed the service to know the name and location of every file available for download, the Court found that Napster did have the ability to police its network, and concluded that it was liable for vicarious infringement.

This argument fails when applied to current peer-to-peer networks. Since they are truly decentralized, they are ignorant of what files their users have chosen to exchange. Other then well- placed warnings; decentralized peer-to-peer networks simply do not have the means to police their network. Furthermore, since the Court in *Napster* made it clear that the duty to police a peer-to-peer network only goes as far the system's architecture allows[112], then it would appear that decentralized peer-to-peer networks truly have no duty to control their users.

Again, affected copyright holders would still have the option of seeking out infringing files and notifying the network operator of their existence, thus forcing them to take appropriate action against a users account. However, not only would this be burdensome upon the copyright holder, in some cases it would also be ineffective. Currently, there exist an entire category of peer-to-peer networks, led by operators such as Freenet, that do not even require a user to have an account to log on.[113] With this particular group of operators, reporting infringing files to them would be useless,

because the operator has no control over what a user chooses to do with their software.

C. Conclusion on the Napster Decision

If the record industries purpose behind filing suit against Napster was to set a controlling precedent that would halt peer-to-peer file sharing, they may have failed. There is a very good chance that the *Napster* decision was obsolete before it even came out. By removing central servers from their architecture, peer-to-peer networks may have easily put themselves beyond the reach of the *Napster* decision. In a strange twist, they may have finally transformed themselves from network operators into what they have always claimed to be, software distributors.

VI. Conclusion

By the incredible amount of copyrighted materials currently online, its safe to conclude that the entertainment industry has failed to stem the flow thus far. This failure is probably directly related to the apparent failure of their attempted legal solution to the problem of peer-to-peer file sharing.

The entertainment industries' legal battles against peer-to-peer networking is evidence that legal solutions are sometimes inappropriate for issues involving technology. In the digital age, technology simply moves too fast and, apparently, courts are unable to keep up. The Napster quandary has shown that because of the almost infinite demand for entertainment over the Internet, even if the entertainment industry were able to shut down the current crop of peer-to-peer networks, something else would rise and quickly take its place.

The entertainment industry should strongly consider alternative solutions to the growing problem presented by peer-to-peer networks. Some commentators have suggested a technology approach using advanced encryption so that the owner may no longer transfer music or movies to their computers.[114] However, this approach has raised concerns about how consumers would react to no longer be able to copy CD's they have legally bought.[115] Alternatively, the entertainment industry could adopt a business approach and begin operating their own peer-to-peer subscription services for a reasonable fee. This would allow registered users to access Napster-like services and legally download a variety of music files. Although this seems like the perfect compromise, there is some dispute on whether the companies who currently control the music industry would be able to make the same profits through peer-to-peer distribution as they do on their current retail store model of distribution.[116]

Whatever solution the entertainment industry decides to adopt, it should begin with the assumption that peer-to-peer file sharing is not going anywhere. Napster has whet the appetite of millions of consumers, and now there exist a demand to be able to obtain entertainment files over the Internet. If record companies continue to ignore this huge market they will inevitably suffer.

Economists make much of the historical fact that the pony express, went out of business within weeks of the first telegraph message. Unless the entertainment industry is willing to bring its distribution methods of music and movies into the 21st century, they may soon find themselves in the same precarious situation.

Footnotes

1 See generally A&M Records, Inc. et al. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

2 Vickie L. Feeman Et Al., Revenge of the Record Industry Association of America: The Rise and Fall of Napster, 9 Vill. Sports & Ent. L.J. 35 (2002).

3 See A&M Records, 284 F.3d 1091 (9th Cir. 2002)(A later Napster decision finally granting the preliminary motion considered by earlier Napster decisions.)

4 The label "operator" is used because of a lack of a better term to describe the role that targeted companies play in the peer-to-peer file-sharing process. It is not meant to overemphasize their part in the process.

5 Metro-Goldwyn-Mayer Studios Inc., et al. v. Grokster Ltd. et al., 243 F.Supp.2d 1073 (C.D. 2003).

6 Id.

7 In actuality there were at least four opinions released regarding the Napster litigation. This article mainly relies on the first opinion by the Federal District Court cited as A&M Records v. Napster, 11 F.Supp.2d 896 (N.D. Calf. 2000), and the first Ninth Circuit Court of Appeals decision cited as A&M Records v. Napster, 239 F.3d 1004 (9th Cir. 2001). For the convenience of the reader these cases will be respectively referred to parenthetically as "Napster I" and "Napster II".

8 Metro-Goldwyn, 243 F.supp.2d. at 1089-93.

9 E.g. Id. at 1081. (One of the issues the Court reviews is whether one of the Defendant's recent re-incorporation in the island nation of Vanatu puts it beyond the court's jurisdiction. Presumably this step was taken by the Defendant for the purpose of avoiding liability under U.S. Copyright law.)

10 Robert Kwant, The Legality of Music City, Kazaa, and Grokster in the Wake of the Napster Decision, 2002 UCLA J. L. & Tech. 10 (2002). (Page numbers are currently not available for this article.)

11 Timothy James Ryan, Infringement.com: RIAA v. Napster and the War Against Online Music Piracy, 44 Ariz L. Rev. 495, 496 (2002).

12 Id.

13 Id.

14 Id.

15 Id.

16 Id.

17 Damien A. Riehl, The Peer-to-Peer Distribution Systems: Will Napster, Gnutella, and Freenet Create a Copyright Nirvana or Gehenna, 27 Sm. Mitchell L. Rev. 1761, 1764-66 (2001).

18 Id.

19 Id.

20 Id.

21 Id.

22 Id.

23 Riehl, supra note 17, at 1766-67.

24 Kwant, supra note 10.

25 Id.

26 Id.

27 Id.

28 Id.

29 Id.

30 Kwant, supra note 10.

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

32 See generally, 17 U.S.C. § 101-1332 (1994 & Supp. V 1999). See also, Gershwin Publishing Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1161-62 (2d Cir. 1971)("Although the [Copyright] Act does not specifically delineate what kind or degree of participation in an infringement is actionable, it has long been held that one may be liable for copyright infringement even though he has not himself performed the protected composition.")

33 Sony Corp. of Am. V. Universal City Studios, Inc., 464 U.S. 417, 435 (1984).

34 Fonovisa, 76 F.3d 259, 264. (citing 2 Nimmer § 1204(a)(2))(In general this section contains an excellent explanation of the basis and application of the claim of contributory copyright infringement.)

35 Timothy James Ryan, Infringement.com: RIAA v. Napster and the War Against Online Music Piracy, 44 Ariz. L. Rev. 495, 504 (2002).

36 See Fonovisa, 76 F.3d 259.

37 Id. at 260-62.

38 Id.

39 Id. at 264.

40 See generally Religious Technology Center v. Netcom On-Line Communication Services, Inc., 907 F. Supp. 1361 (N.D.Cal. 1995).

41 Id. at 1371.

42 Id. at 1374.

43 A&M Records, 239 F.3d 1004, 1021. ("We agree that if a computer system operator learns of specific infringing material available on his system and fails to purge such material from the system, the operator known of and contributes to direct infringement.")(Napster II)

44 E.g., Id. at 1020-23. (The Defendant, Napster, was ultimately found guilty of contributory infringement, however, liability was based on damaging documents indicating that Napster had actual knowledge of the infringement taking place on its peer-to-peer Network. In fact, in the same section the Court concluded that Napster was indeed guilty of contributory infringement is also stated that "[w]e . . . will not impute therequisite level of knowledge to Napster merely because peer-to-peer file sharing technology may be used to infringe plaintiffs' copyrights." The Court of Appeals went on to also hold that "in an online context, evidence of actual knowledge of specific acts of infringement is required to hold a computer system operator liable for contributory copyright infringement." [Emphasis added]

45 Fonovisa, 76 F.3d at 261-64.

46 Dan Dobbs, The Law of Torts § 333 (2001).

47 The Court in Gershwin, probably one of the leading cases involving vicarious copyright infringement, carefully reviewed this test and stated: "one may be vicariously liable if he has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities." Gershwin Publishing Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (2d Cir. 1971).

48 See generally, Shapiro, Bernstein & Co., Inc., et al. v. H. L. Green Co., Inc., et al., 316 F.2d 304 (2cd Cir. 1963).

49 Id. at 305-07

50 Id.

51 See e.g., Deutsch v. Arnold, 98 F.2d 686 (2d Cir. 1938).

52 Shapiro, 316 f.2d at 307.

53 Id.

54 Id.

55 Id.

56 Id. at 308

57 Id.

58 Gershwin, 442 F.2d at 1136. (Quote cited above at note 35).

59 See generally, Metro-Goldwyn, 243 F.Supp.2d 1073 (2003).

60 A&M Records, 239 F.3d at 1014. (Court upheld the lower court's ruling rejecting Napster's assertion of fair use as a defense Plaintiffs' claims of indirect liability.) (Napster II)

61 See generally, Sony Corporation of America, et al., v. Universal City Studios, Inc., et al., 464 U.S. 417 (1984).

62 Id. at 442.

63 A&M Records, 239 F.3d at 1022-23. (It should be noted and as the Court in Napster pointed out that the Substantial Use doctrine is not a defense to a claim of vicarious copyright infringement. Although the Sony Court referred to vicarious infringement, it was using the term vicarious in the broad legal sense, and not in reference to the specific claim of vicarious copyright infringement.) (Napster II)

64 Id. at 439.

65 Id. at 420.

66 Id.

67 Id.

68 Sony, 464 U.S. at 439.

69 Id. (The Court went so far as to refer to the "historic kinship" between patent and copyright law.)

70 Id. (Quoting Henry v. A.B. Dick Co., 224 U.S. 1, 48 (1912).)

71 A&M Records, 114 F.Supp.2d at 916-17. (Napster I)

72 Pub. L. 105-304, 112 Stat. 2860 (1998).

73 Corey Rayburn, After Napster, 6 Va. J.L. & Tech. 16, 34 (2001). ("Many commentators viewed the [DMCA] as Congress shifting the law from the protection of original works to the maximization of the recoding industry's profits.")

74 42 U.S.C 512(a)

75 See generally 42 U.S.C. 512. (The immunity set forth in 512(a) is subject to the conditions set forth throughout section 512.)

76 Rayburn, supra note 73.

77 A&M Records, 239 F.3d at 1025. (The Court of Appeals left open the issue of whether a peer-to-peer network such as Napster would fall under the DMCA definition of service provider. Instead the Court concluded that " plaintiffs raise serious questions regarding Napster's ability to obtain shelter under § 512[.]")(Napster II)

78 42 U.S.C. 512(k)(1).

79 Hisanari Harry Tanaka, Post-Napster: Peer-to-Peer File Sharing Systems Current and Future Issues on Secondary Liability Under Copyright Laws in the United States and Japan, 22 Loy. L.A. Ent. L. Rev 37, 54 (2001).

80 A&M Records v. Napster, 2000 WL 573136 at *10 (N.D.Cal 2000).

81 Id.

82 In re: Aimster Copyright Litigation, 2002 WL 31006142 at *20 (N.D.Ill. 2002).

83 A&M Records, 239 F.3d at 1013. (It is important to note that all of the claims discussed were being reviewed in order to determine if a preliminary injunction should be issued. Accordingly, plaintiffs were only required to prove probable success on any of the claims discussed herein.)

84 Ryan, supra note 29 at 500.

85 Id. (The original co-authors of the Napster software were Sean Parker and Jordan Ritter.)

[86] Id.

[87] Id.

[88] Id. (Fanning picked up the childhood nickname due to his unkempt hair due.)

[89] Ryan, supra note 11 at 500-01.

[90] Id.

[91] A&M Records, 114 F. Supp. at 902. ("[Napster] eventually plans to 'monetize' [sic] its user base. Potential revenue sources include targeted email; advertising; commissions from links to commercial websites; and direct marketing of CDs[.]") (Napster I)

[92] A&M Records, 114 F.Supp. at 900. (Napster I)

[93] Id. at 900. (Plaintiffs also claimed that Napster was also guilty unfair competition, however, that claim will not be discussed in this article.)

[94] Gershwin, 443 F.2d at 1162.

[95] A&M Records, 239 F.3d at 1020-21.(Napster II)

[96] Id.

[97] Gershwin, 443 F.2d at 1162.

[98] A&M Records, 239 F.3d at 1024. (Napster II)

[99] Id. at 1023.

[100] Id. at 1023-24.

[101] Id.

[102] Id.

[103] A&M Records, 239 F.3d at 1023-24. (Napster II)

[104] Id. at 1023.

[105] A&M Records, 114 F.Supp.2d at 902. (Napster I)

[106] A&M Records, 239 F.3d at 1023. (Napster II)

[107] Id. at 1021.

[108] Id. at 1020.

[109] Id. at 1021.

[110] Id. at 1023.

[111] Id.

[112] Id. at 1023-24.

[113] E.g. Riehl, supra note 17 at 1779-80. ("What makes Freenet more threatening than its [peer-to-peer] cousins is its devoition to keep the source of the information passing through its system absolutely anonymous.")

[114] Grace J. Bergen, The Napster Case: The Whole World is Listening, 15 Transnat'l Law. 259, 273-74 (2002).

[115] Id.

[116] See generally Peter Jan Honigsberg, The Evolution and Revolution of Napster, 36 U.S.F. L. Rev. 473 (2002).

Ed Langs Writing Awards

The following are the winners of the Computer Law Section 2003 Writing Contest.

First Place Winner

George Pitchford
Southfield, Michigan 48034

System Failure: Has the A&M v. Napster Decision Been Rendered Obsolete in the War Against Peer-to-Peer File-Sharing Networks?

Second Place Winner

JoAnne Williams
Bloomfield, Michigan 48304

P2P Models: Napster and its Impact on Subsequent and Future of File Sharing on the Internet

Third Place Winner

Maisa Kharbush
Livonia, Michigan 48152

The TEACH Act: A History Of The Technology, Education, and Copyright Harmonization

E-Mail Marketing

- Lawmakers on Attack Part II

by John J. Genord, Esq.

In March of 2003, I wrote an article entitled E-Mail Marketing - Lawmakers on Attack,which centered around House Bill 4188, seeking to amend the Michigan Consumer Protection Act to curb abusive tactics employed by some email marketers. This is a follow-up on that article.

House Bill 4188 as was stated in my previous article, was referred to the Energy and Technology Committee in the House of Representatives. Unfortunately, after that, it did not receive much discussion, according to Representative Marc Shulman.

Another bill, however, was introduced in July of 2003, which sought to create the Unsolicited Commercial E-Mail Protection Act. It was passed into law and became effective on September 1, 2003. This act has several requirements and prohibitions regarding unsolicited commercial email. The Act applies to any unsolicited commercial email sent to a Michigan resident or through a Michigan e-mail service provider.

Among the requirements are the following. Section 3 of the Act requires the email to contain certain information:

> (A) the subject-line must start with the characters "ADV:". This will permit properly configured spam filters to sort out unwanted advertising email. A company's IT-person or service provider will be able to assist with this.
>
> (B) the e-mail must conspicuously include the street address of the sender, the legal name of the sender, the valid internet domain name (i.e., genordlaw.com) and the sender's valid e-mail address for return correspondence. It is all-too-common that abusive advertisers manipulate and disguise the source information and email address.

Often times, the recipient cannot even reply to the sender. This new law seeks to curb that abusive practice. (C) the e-mail must also include specific opt-out language and an easy manner in which the recipient may request, either electronically or by way of a toll-free number, to be taken off of the list.

The Act also prohibits certain conduct. Among other things, it prohibits disguising the sender's email address or otherwise obscuring where the correspondence originated from. It also prohibits the use of a third-party's domain name as identifying the point-of-origin without their permission. This has been another common practice. The thought behind this practice of the mischievous advertisers was that a popular domain name would make recipients more likely to open the email. True? Maybe. Deceptive? Yes. And now, illegal? Absolutely.

The Act provides for a civil cause of action for recipients of such emails as well as any internet service provider through whose network such an email was transmitted. In addition, the Attorney General may bring an action. Moreover, violations are either misdemeanors or felonies depending on their nature. Statutory damages range from $500.00 to $250,000.00 and more!

This act is a good step toward curbing abusive practices, however, it does not address another abusive practice: misleading content. This is why the Consumer's Protection Act should be amended in order to prohibit misleading content. An advertiser should not only be required to put ADV: at the subject-line, but should not be permitted to include misleading information in the subject-line (or the body of the email) following that disclaimer.

While I am all for e-mail marketing, as it permits (because of its relatively low cost) the smaller players to compete with the larger companies, because of the abusive conduct of many advertisers, limits need to be set and there is more work to do. If your clients are considering an email marketing campaign in Michigan, they need to be aware of the Unsolicited Commercial E-mail Protection Act. Public Act 42 of 2003.

John J. Genord is an attorney practicing in the areas of collections and commercial litigation. He can be reached at john@genordlaw.com for more information.

State Bar of Michigan
Michael Franck Building
306 Townsend Street
Lansing, MI 48933

**Presorted
First Class Mail
U.S. Postage Paid
Lansing, MI 48933
Permit No. 191**