Jurisdictional Statement

This action is a consolidation of multiple lawsuits that were consolidated by order of the Judicial Panel on Multidistrict Litigation pursuant to 28 U.S.C. §1047. The District Court has subject matter jurisdiction over the matter pursuant to 28 U.S.C. §§ 1331, 1338. The District Court entered its preliminary injunction order on October 30, 2002, and Appellant John Deep filed a timely Notice of Appeal on November 27, 2002. This Court has jurisdiction over the appeal pursuant to 28 U.S.C. §1292.

Statement of the Issues on Appeal

1. Whether the District Court improperly resolved disputed issues of material fact in issuing a preliminary injunction without holding an evidentiary hearing.

2. Whether the District Court committed an error of law by failing to apply the correct legal standard for contributory copyright infringement required by *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984).

3. Whether the District Court properly extended the doctrine of vicarious copyright infringement to the private instant messaging software at issue in this case.

4. Whether the District Court properly found that the Safe Harbor Provisions of the Digital Millenium Copyright Act, 17 U.S.C. §512, do not apply in this case.

5. Whether the District Court properly construed the factors required for the issuance of injunctive relief.

6. Whether, if injunctive relief was in fact warranted here, the injunction issued by the District Court was overbroad and impermissibly vague by restraining legitimate activity outside the scope of the injunction hearing and broadly directing the enjoined parties not to infringe plaintiffs' copyrights.

Statement of the Case

As set forth in the Jurisdictional Statement above, this case is a consolidation of several actions for contributory and vicarious copyright infringement against AbovePeer, Inc., Buddy USA, Inc., and Appellant John Deep (collectively hereinafter the "Defendants"). In December 2001, certain plaintiffs moved for a preliminary injunction, and the parties filed their respective briefs and supporting declarations.

In April and May 2002, the Defendants filed bankruptcy petitions in the Northern District of New York, thereby invoking the automatic stay provisions of 11 U.S.C. §362 of the Bankruptcy Code. Appellees moved for relief from the stay in each bankruptcy so that the district court in this case could rule on the then-

pending motion for a preliminary injunction in this action. In arguing for such relief, Appellee impressed upon the bankruptcy court (over the debtors' strong objections) that no evidentiary hearings would be necessary, that the matter was fully briefed, and that the only expense the bankruptcy estates would incur would be "a ticket on Southwest Airlines for special counsel to go to Chicago" for arguments. (Bankr. Transcript, May 28, 2002, at 39:13-14.) Moreover, Plaintiffs made clear to the bankruptcy court that the preliminary injunction, if granted, would not terminate the use of the Defendants' technology:

> And I think what is equally important to this Court in exercising your discretion is what it is -- to focus exactly what it is that we are asking Judge Aspen to do in the preliminary injunction. *We have not asked Judge Aspen to enjoin the technology.* We have not asked Judge Aspen to do anything with the source code . . . . What we are asking Judge Aspen to do is to issue an injunction that prevents infringement. We're not talking about a technology. We're not talking about source code. That's a red herring. We're talking about a business plan that was designed and implemented specifically for infringement. It wasn't implemented or designed for instant messaging. *[The debtor] can do all the instant messaging he wants.*

(Bankr. Transcript, May 28, 2002, at 24:22 – 25:11; emphasis added.) The Bankruptcy Court thereafter permitted limited relief from the stay, concluding that the District Court in Chicago could render its decision only if it could do so without the necessity of an evidentiary hearing. *In re Deep, et al*, 279 B.R. 653, 659 (Bankr. N.D.N.Y. 2002).

The parties at that point had not taken even limited discovery, an option that the bankruptcy court's limited stay relief likewise now foreclosed. Thus, having only the parties' moving papers and supporting declarations to consider – all of which

had been filed five months earlier without knowledge that an evidentiary hearing would later be foreclosed -- the district court entertained a brief oral argument and issued its opinion granting the motion. (Memorandum Opinion and Order, Sept. 4, 2002, (hereinafter "Opinion").)

After issuing its Opinion, the district court requested that Appellees submit a proposed Preliminary Injunction. The Court entered Appellees' proposed injunction order over Defendants' objections without change. (Preliminary Injunction Order, Nov. 1, 2002 (hereinafter "Preliminary Injunction Order").)

After Mr. Deep filed the Defendants' first required Compliance Report stating, in effect, that the broad terms of the Preliminary Injunction could not be accomplished within the architecture of the system (First Report of Compliance, Nov. 12, 2002), Appellees moved for an order to show cause why the Defendants should not be held in contempt. In their motion, Appellees stated:

> Appellees bring this Motion for Order to Show Cause re Contempt seeking the appointment of a compliance officer to that which this Court already has ordered Defendants to do: shut down the Aimster System and Service until Defendants comply with the Preliminary Injunction Order.

(Memorandum in Support of Appellees' Motion For Order to Show Cause Re Contempt, Nov. 20, 2002, at 1.) In response to the Defendants' contention that they could not comply with the terms of the injunction, Appellees argued that the injunction could be followed in one very simple way: shutting down the entire system – the very relief that they had previously represented to the Bankruptcy Court they would not seek. (Memorandum in Support of Motion For Order to Show

Cause, Nov. 20, 2000, at 6 - 7.)

On November 26, 2002, the district court heard Appellees' motion for an order to show cause. At the hearing, Appellees again asked the court to shut down the Defendants' business and terminate any use of technology:

> The Court's order is clear, there's no dispute about that. The defendants have not shut down, as the order requested. They haven't tried to filter, as the order requested. The result is, as we have placed before your Honor, continued countless infringements of complaint works, of billboard works, new works, new releases, others. Infringement is multiplying at this, the very height of the pre-Christmas season, when our clients are attempting to sell their product.

(Hearing Trans. Nov. 26, 2002, at 2:21 – 3:13.) The district court then ordered Defendants to show cause why they should not be held in contempt. In addition, at the request of Appellees, the court indicated that it would issue a temporary restraining order in the meantime, and it asked Appellees to tender such an order. Appellees' proposed order, which was signed and entered by the district court over the Defendants' objections on December 2, required the Defendant not only to shut down the instant messaging system at issue in the case, but also to disconnect all Defendants' computers and terminate all access to the Internet:

> 1. Aimster immediately shall disable and disconnect any and all computers, including servers, used in connection with the website, server, hardware, software, or any other system or service owned or controlled by Aimster (the "Aimster System and Service") including those located at 80 State Street, Albany, New York.
>
> 2. Aimster immediately shall terminate all Internet access for the Aimster System and Service. Within three (3) days of entry of this Order, Defendants shall give written notice and a copy of this Order to any and all providers of Internet access for the Aimster System and Service, including without limitation, Internet access

provided by Qwest Communications International, Inc.

(Temporary Restraining Order, Dec. 2, 2002, at ¶¶ 1 – 2.) When issuing the TRO, the District Court noted, "I simply am reiterating, if not the same language, the clear intent of the preliminary injunction that was granted before." (Hearing Transcript, Nov. 26, 2002.)

Statement of the Facts

Instant messaging is a popular form of communication over the Internet. The District Court's opinion described standard instant messaging in the following manner:

> Instant messaging ("IM") is a way for people to communicate instantly over the computer to one or more 'buddies' that they specify. *See generally,* Mujica Decl. PP5-7. There are several different IM networks, including America Online's Instant Messenger ("AOL IM"), ICQ, and Yahoo IM. Instant Messaging works through the use of a computer program that each individual user downloads to his or her machine. With the program installed, the computer connects to the IM network and the user can specify friends that also have the IM program installed on their computers. The system then alerts the user in real time whenever those friends are online. When a friend is online, the user can send that person an instant message that will pop up on their screen. The users can then chat back and forth in real time using their keyboards. As such, instant messaging is much faster than e-mail. An instant message pops up on the screen unbidden as soon as it is sent from a friend's computer.
>
> AOL IM also has a feature that allows buddies to transfer files to each other. There are two ways a AOL IM user can transfer files: by using a file transfer or AOL IM's "get file" functionality. A simple file transfer on AOL IM requires a user to specify a file on his hard drive to send to one of his IM buddies. The buddy, after signaling his acceptance of the transfer, would then receive the file onto his hard drive. This method of file transfer can be used to send any kind of files over the AOL IM network, including documents, digital pictures, and MP3 music.

> Another aspect of AOL IM's file transfer feature is the "get file" functionality. This function is the ability of a user to specify certain files or directories that are available for other users to freely take at their leisure. So, for instance, if an AOL IM user wanted to allow his friends to download any of the pictures located on his computer, he would simply specify to the AOL IM program that those buddies have access to those files. Anytime thereafter, the buddies could retrieve those files. That is, the user does not have to actually send those files to his buddies; the buddies could, rather, retrieve the files for themselves.

(Opinion at 4 – 5; *see also* Supplemental Declaration of John Deep, February 13, 2002, describing functionality of AOL instant messaging system.)

The Defendants' private instant messaging was a kind of instant messaging that relied on encryption to let users communicate with "buddies" in a private, encrypted network. (Declaration of John Deep In Opposition to Plaintiffs' Motion For a Preliminary Injunction, Jan. 22, 2001 (hereinafter "First Deep Declaration") at ¶¶ 3– 6.) The encryption functionality was necessary for the creation of truly private networks because otherwise, as with non-encrypted instant messaging, imposters outside a buddy group could have access to communications within the buddy group.

The private instant messaging involved two basic components. First, users had to install the messaging software, which could be obtained for free at www.aimster.com or through other online sources from which "freeware" is distributed. (Declaration of Katherine B. Forrest, Dec. 20, 2001, (hereinafter "Forrest Declaration"), Ex. 1.) After installing the software, users could choose a "buddy list" from which a private network was instantly created for sharing encrypted messages of all kinds, including text, user profiles, and files.

Second, the Defendants provided certain routine "backbone" infrastructure elements, such as caching servers that made text communications between the users work better. (First Deep Declaration at ¶¶ 11 – 14.) However, these backbone services were not a proprietary network, and thus the messaging software could continue to function even if the Defendants did not provide those services. (Deep Decl., Oct. 17, 2002, at ¶¶ 10 – 11.)

The District Court provided the following description of the Defendants' private instant messaging:

> According to Deep, Aimster performs two fundamental functions. *See generally,* Deep Decl. PP 4-6. First, it allows its users to send messages or transfer files to other users by facilitating the creation of direct user-to-user (or peer-to-peer) networks. Through the use of encryption technology contained within the Aimster software, the individual users are assured of complete privacy in their online transaction. In particular, Deep claims that Defendants have no knowledge whatsoever of when its users are exchanging files, who are exchanging files, or what files are being exchanged. Deep Decl. P 4. Aimster encrypts all the information that is transferred between its users on their private networks. Even the identities of such users are encrypted. Deep Decl. P 8. While Deep admits that Aimster can be used to transfer musical works (just as it can be used to transfer any other information or data) from one user to another, the subject matter of the transfer and the recipient are determined entirely by the users themselves. Deep Decl. P 10. In short, Defendants go to great pains to characterize the Aimster service as merely an innocent provider of "infrastructure services" to end users, *Id.,* with the implication being that Aimster is not and should not be held responsible for the malfeasance, if any, of its end users. According to Deep, virtually all "of the copyrighted musical works that Plaintiffs claim are being infringed by Defendants are songs that are transferred by individual users from one hard drive to another using Aimster solely as an internet service provider, in much the same way that such files can be and are transferred on AOL and other internet service providers." Deep Decl. P 22.
>
> Aimster's second fundamental function, according to Deep, is to allow users to identify other "buddies" who have similar interests and

> who may wish to correspond and exchange files. Deep Decl. P 5. Users of the Aimster system locate buddies by searching the user profiles on the system. The user profile identifies other users by subject matter of interest or "by the name of the file or files that user has available on his or her hard drive." *Id.*

(Opinion at 5 - 6.)

A more detailed description of the private messaging software and the optional infrastructure services provided by the Defendants is set forth in the January 22, 2001, Declaration of John Deep at ¶¶ 3 – 23. Among other things, that declaration establishes the following material facts:

> 8. As stated, Aimster encrypts all the information that is transferred between users. Accordingly, Aimster contains only encrypted references to the computers or physical addresses where digital files are stored. Even the identities of the users are encrypted. Indeed every communication between and among the users is encrypted. Just like an electronic bank transaction or other financial transaction, only the parties to the transaction have access to the transmission.
>
> 9. In this sense, Aimster merely provides infrastructure services to users. The users themselves control the transaction.
>
> 10. While Aimster can be used to transfer musical works (like any other information or data) from one user to another, the subject matter of the transfer and the recipient are determined entirely by the users. If Aimster users wish to exchange among themselves electronic data representing literal or musical works they choose from a list of "buddies" who have themselves chosen to list what files they have available on their buddy list.
>
> 11. As an infrastructure provider, Aimster . . . . does not deal directly with end users. Instead, it provides services to end users only by relying on intermediate contractual relationships with other internet service providers who, in turn, may act as intermediate service providers or may act as primary internet service providers and have direct commercial relationships with end users.
>
> 12. Aimster does not request or store the personal identity of the end user or their email address or their internet protocol address.

> Because all that information is encrypted, Defendants have no knowledge of a user's log-in name or identity.
>
> 13. In many respects, Aimster operates in the standard way that many infrastructure providers do, such as providers of email gateways, instant messaging, and caching servers. Aimster provides the backbone that allows end users to communicate with one another. Accordingly, the architecture of Aimster is based on standard instant messaging technology and is nearly identical to the architecture of other internet service providers such as Plaintiff AOL's instant messaging service.

(First Deep Declaration at ¶¶ 7 – 13; *see also* Declaration of John A. Deep in Opposition to Plaintiffs' Proposed Preliminary Injunction Order, Oct. 17, 2002, at ¶¶ 3 – 15, 23; Forrest Declaration, Ex. 1 – Aimster Tutorial.)

The record therefore reflects that, after the user had acquired the private messaging software, the Defendants did not have direct contact with any user and, significantly, could not know or control the identity or activities of any user – including whether those users continued to use the Defendants' servers. While certain aspects of any communications between users passed through the Defendants' servers, the private messaging software encrypted all aspects of any communication before the communication left the user's computer. And the communication reached the Defendants' servers only indirectly by first passing through the user's internet service provider (and possibly other service providers). As a result of the user's encryption of the communications, the *only* thing that the Defendants could somehow "see" (and therefore even arguably control) was an ongoing stream of jibberish coming from multiple unidentified sources.

A separate part of what the District Court referred to when speaking elsewhere in its Opinion about "Aimster" consisted of certain websites, which were available to the general public regardless of whether the person visiting the websites had installed the private instant messaging software. One website – www.aimster.com -- permitted downloads of the messaging software, provided news and links to a separate website (http://forums.aimster.com) with forums in which visitors could post comments and otherwise communicate with each other, had a Help section and a tutorial, and set forth information about copyright and privacy rights. (Forrest Decl. Exs. 1, 3, 4)

A second website – www.clubaimster.com -- provided an online magazine that listed the "Aimster Top 40," which was a list compiled by mining anonymous user data. (Reply Declaration of Katherine B. Forrest, Feb. 4, 2002, (hereinafter "Forrest Reply Declaration") Ex. 3 at pp. 248 – 53; First Deep Declaration at ¶ 21.) If a Club Aimster member also had installed the appropriate searching software (software known as "Club Aimster Software" and based on the "Mailster" protocol), he or she could click on one of the listings in the Top 40 and the software would perform a search within a certain "buddy group" using the listing as a search term. (Decl. of Katherine B. Forrest, Ex. 19B; Forrest Reply Declaration, Ex. 3 at pp. 248 – 53; First Deep Declaration at ¶ 21.) The Club Aimster website did not interoperate, however, with the Aimster instant messaging software, and there is no evidence in the record to suggest otherwise.

In later parts of its Opinion, the District Court reached certain erroneous factual conclusions concerning the technology at issue. Much of the court's confusion was due to its misunderstanding of the disparate nature of the software used for private instant messaging and the various Internet websites, which operated using web technology. First, and most significantly, the District Court apparently confused the sign-in page for Club Aimster with the log-in for users of the private instant messaging software. The Court's opinion provides:

> Plaintiffs have provided defendants with screen shots of the Aimster system showing the availability of Plaintiffs' copyrighted sound recordings on those users' hard drives. Forrest Decl. Ex. 20. The screen shots unequivocally identify the individual users ("buddies") who possess the offending files. *Id.* Each of these individually identified users must log on to the Aimster system with a password and user name provided by Aimster. Forrest Decl. Ex. 19 (screen shot of the Aimster login screen). While it may be true that the actual transfers between users are unknown to Defendants due to Aimster's encryption scheme, it is disingenuous of Defendants to suggest that it is unaware of which users are using its system and what files those users are offering up for other users to download at their whim.

(Opinion at 22-23.) The screen shots in Forrest Ex. 20 are screen shots of the instant messaging software, which show the user names (e.g., Mi652, Witti15, tacito 168) of the individuals sharing user profiles. As stated in Mr. Deep's declarations, due to the private nature of the networks created by the users and the encryption of all user information by the user, those user names could not be matched up to particular users. Therefore, unless Mr. Deep could somehow decrypt the encrypted information,[1] he could not know whether any particular user was logging-in to use

[1] Just as a lock maker without a key cannot unlock a lock he has made, a provider of encryption software cannot decrypt an encrypted message or file without the encryption key. The encryption and decryption keys employed by private messaging

the instant messaging software, communicating with another user, or transferring files. (First Deep Declaration at 8 – 12; Declaration of John A. Deep in Opposition to Plaintiffs' Proposed Preliminary Injunction Order, Oct. 17, 2002, at ¶¶ 7 – 9.) The sign-in page included in Forrest Ex. 19 was a sign-in for something completely different – a "members only" webpage that was part of Club Aimster. As the screen shot in Forrest Ex. 19 (referred to by the District Court) reflects, the "member name" for signing in to Club Aimster was the member's e-mail address. And because a person's "user name" for the software was different than his or her "member name" (i.e., email address) for Club Aimster, there simply was no way to correlate the two.

Another fundamental error – again based on apparent confusion between the instant messaging software and the separate website activities – was the Court's conclusion that Aimster's "repeat infringer policy" could not be implemented due to the encryption functionality of the instant messaging software. The "repeat infringer policy" to which the Court referred – Aimster's Copyright Notice page in

---

users were known only to the users themselves, not to Mr. Deep. (Declaration of John Deep at ¶¶ 3 – 15.). As such, it would have been virtually impossible from a technological standpoint for Mr. Deep to decrypt user communications.

Moreover, the software's encryption functionality would in many cases constitute a "technological measure that effectively controls access to a work protected" by the Copyright Act under the terms of the anti-circumvention provisions of the Digital Millennium Copyright Act. *See* 17 U.S.C. §§ 1201(a)(1)(A), (2)(B). Thus, even if possible, any efforts to circumvent that technological measure by trying to decrypt the encrypted messages and attached files would quite likely constitute a violation of § 1201(a) of the Copyright Act. Similarly, decryption of user messages and attached files, if feasible, would likely violate the Electronic Communications Privacy Act, as the interception of electronic communications. *See* 18 U.S.C. §§ 2511, 2512.

Forrest Decl. Ex. 8 – applied to the entire website, including the many forums available for use by visitors to the website. (*See* Forrest Decl. Exs. 9 – 12 for screen shots of forums in which visitors were free to post messages, comments, etc.) If properly notified of infringing content being posted in the forums or other portions of the website, Aimster could and would take appropriate steps as required by the Digital Millennium Copyright Act. The District Court, however, mistakenly concluded that the policy was impossible to implement (and therefore was not a "reasonable implementation") because the Court looked only at possible infringement through use of the instant messaging software. Because infringement using the instant messaging software could not be policed, the Court concluded that "[a]dopting a repeat infringer policy and then purposely eviscerating any hope that the policy could ever be carried out [was] not an 'implementation' as required by [17 U.S.C.] § 512(i)." (Opinion at 36 – 37.) Since the Court mistakenly looked only to the instant messaging software and not the website, its conclusion was in error.

Another instance in which the District Court appears to have been confused was the Court's conclusion that, because it considered the private instant messaging networks to be "peer-to-peer" systems, all communications between users went directly from one user to another without ever going "through" Aimster for purposes of 17 U.S.C. § 512(a). (Opinion at 37.) While that was correct with regard to actual file transfers, it was not correct for user profile searches, instant messages, chat, and other communications between users. (First Deep Declaration at ¶¶ 13, 14, 19.) Indeed, the District Court itself states in a later part of its Opinion that

Aimster had "provide[d] ample explanation of how and why certain information is cached on their system." (Opinion at 38.) The Court goes on to recognize in a footnote that Mr. Deep's declaration specifically addressed the caching of "data," "messages," and "attributes," but did not claim that caching of file transfers occurred. "Caching" is term that refers to the temporary storage of computer data on a digital medium, such as a server (as is the case here).

The District Court also failed to recognize that "the creator of each private network has the ability to limit access to its network to as many users as it desires" (First Deep Decl. ¶ 4) and that "[i]f a network is created, information can be exchanged in encrypted form." (First Deep Decl. ¶ 5). Instead, the Court found that "Aimster greatly expands the file transferring capability of AOL IM described above by designating every Aimster user as the "buddy" of every other Aimster user. In this way, every Aimster user has the ability to search for and download files contained on the hard drives of any other Aimster user (provided that the user has previously designated those files to be available for searching)." (Opinion at 7.) This finding is in direct contravention of the record as stated above.

Further, while the Court agreed that "Aimster encrypts all the information that is transferred between its users on their private networks" (Opinion at 6), the Court failed to consider how encryption worked, or could work, to make private messages and file attachments accessible to certain users, but not to all users. In fact, the Court did not define its understanding of encryption at all, either by reference to other cases or in its own reference to the record. And yet the Court found that it was

"disingenuous of Defendants to suggest that they lack the requisite level of knowledge when their putative ignorance is due entirely to an encryption scheme *that they themselves put in place*." (Opinion at 23.) In making this finding, the court simply failed to understand, or even to attempt to define, what an "encryption scheme" is, and offered no rationale at all for its finding – in particular, for whether a private messaging software, which relied on encryption to create private networks, could or should plausibly achieve its primary purpose of private messaging other than by relying on encryption.

Finally, the Court failed to understand if or under what circumstances a file attachment could be "available for download", especially if, as the court conceded, "Aimster encrypts all the information that is transferred between its users on their private networks." (Opinion at 6.) As the record reflected, only "the parties to the transaction have access to the transmission." (First Deep Decl. ¶ 8.) This crucial fact distinguishes encrypted private networks from non-encrypted public networks, such as AOL's IM. Thus, the court failed to understand that because "Aimster encrypts all the information that is transferred between its users on their private networks," it follows that users *never* distributed or made "available for download" *any* unencrypted copyrighted content, but at most made available for download only encrypted gibberish.

Summary of the Argument

The District Court erred in granting preliminary injunctive relief for a number of reasons. First, the Court made critical factual errors about highly

complex computer software and internet technology without the benefit of an evidentiary hearing and in direct contradiction to the documentary evidence proffered by the Defendants. Second, the Court misapplied the judicially created doctrines of contributory and vicarious copyright infringement, holding in error that the United States Supreme Court decision in *Sony Corporation v. Universal City Studios* was inapplicable to this case. Third, the Court misapplied the statutory safe harbors provided by the Digital Millennium Copyright Act. Finally, even if injunctive relief were appropriate here, the extraordinarily broad injunction issued by the District Court amounted to an abuse of discretion.

Statement of the Standard of Appellate Review

A grant or denial of a preliminary injunction is reviewed for abuse of discretion. *See Baja Contractors, Inc. v. City of Chicago*, 830 F.2d 667, 674 (7th Cir. 1987), *cert. denied*, 485 U.S. 993 (1988). This Court has also articulated certain of the contours of what constitutes abuse of discretion in the preliminary injunction setting:

> [A] district court abuses its discretion in issuing a preliminary injunction when it applies an incorrect legal standard in determining the likelihood of success on the merits. Similarly, a failure to observe the substantive or formal requirements for the court's order may constitute an abuse of discretion. Where the district court's error is the very predicate of its order, the order must be reversed as an improvident exercise of the court's discretion.

American Can Co. v. Mansukhani, 742 F.2d 314, 326 (7th Cir. 1984).

"When a court of appeals considers a preliminary injunction order, which should set forth the judge's reasoning under Fed. R. Civ. P. 65(d), the factual

determinations are reviewed under a clearly erroneous standard and the necessary legal conclusions are given *de novo* review." *Lawson Products, Inc. v. Avnet, Inc.*, 782 F.2d 1429, 1437 (7th Cir. 1986). Likewise, when findings of fact and conclusions of law are set forth to ground the grant or refusal of a preliminary injunction, "there is an obligation under [Federal Rule of Civil Procedure] 52 (a) to engage in a comprehensive review of the documentary evidence to determine if clear error has been committed." *Id.* at 1439.

Among the purposes of the Rule 52(a) requirement is "to provide appellate courts with a clear understanding of the basis of the trial court's decision." *Bartsh v. Northwest Airlines, Inc.*, 831 F.2d 1297, 1304 (7th Cir. 1987). For this reason, "the findings of fact must include as many of the subsidiary facts as are necessary to disclose to the reviewing court the steps by which the trial court reached its ultimate conclusion on each factual issue." *Monarch Beverage Co., Inc. v. Tyfield Importers, Inc.*, 823 F.2d 1187, 1192 (7th Cir. 1987) Under Rule 52(a), a party appealing the grant of a preliminary injunction is "entitled to have explicit findings of fact upon which the conclusion of the [enjoining] court was based." *Mayo v. Lakeland Highlands Canning Co.*, 309 U.S. 310, 317 (1940).

In the present case, the injunction issued by the District Court follows verbatim the injunction tendered by the Appellees. Under such circumstances, the terms of the injunction are not entitled to the deference normally accorded an injunction crafted by the District Court's, rather than opposing counsel's, discretion. *See Chicago & NW Transp. Co. v. Railway Labor Exec. Ass'n*, 908 F.2d 144, 149 (7th

Cir. 1990) ("[A] district judge has not only the power but also the duty to refuse to enter a defective injunction even if neither party objects."); *Machlett Laboratories, Inc. v. Techny Indus., Inc.*, 665 F.2d 795, 797 (7th Cir. 1981) ("When as in this case the district court merely adopts verbatim the findings and conclusions of the prevailing party, they may therefore be more critically examined.")

Argument

I. Preliminary Injunction Standard

The proper granting or denial of a preliminary injunction requires a multi-step determination on the part of the court:

> As a threshold matter, a party seeking a preliminary injunction must demonstrate (1) some likelihood of succeeding on the merits, and (2) that it has "no adequate remedy at law" and will suffer "irreparable harm" if preliminary relief is denied. If the moving party cannot establish either of these prerequisites, a court's inquiry is over and the injunction must be denied. If, however, the moving party clears both thresholds, the court must then consider: (3) the irreparable harm the non-moving party will suffer if preliminary relief is granted, balancing that harm against the irreparable harm to the moving party if relief is denied; and (4) the public interest, meaning the consequences of granting or denying the injunction to non-parties.

Abbott Laboratories v. Mead Johnson & Co., 971 F.2d 6, 11-12 (7th Cir. 1992). With a view toward minimizing the cost of error, the four factors are weighed on a sliding scale whereby, for example, a plaintiff's low chance of success on the merits must be countered by a great deal of irreparable harm. *Id.* at 12. A preliminary injunction, however, should do no more than "preserve the status quo"; it should not impose substantial hardship on the defendant. *See Santos v. Columbus-Cuneo-Cabrini*

Medial Center, 684 F.2d 1346, 1350-51 (7th Cir. 1982); *Roland Mach. Co. v. Dresser Indus., Inc.*, 749 F.2d 380, 383 (7th Cir. 1984).

II. The District Court should not have issued a Preliminary Injunction without the benefit of an evidentiary hearing to elucidate the inner workings and interoperation of Aimster's instant messaging software and Aimster's separate websites.

In this judicial circuit, an evidentiary hearing is required to resolve a preliminary injunction motion when material factual issues are disputed. *See Ty, Inc. Inc. v. GMA Accessories, Inc.,* 132 F.3d 1167, 1171 (7th Cir. 1997); *Medeco Security Locks, Inc. v. Swiderek*, 680 F.2d 37, 38-39 (7th Cir. 1981); *General Electric Co. v. American Wholesale Co.*, 235 F.2d 606, 608 (7th Cir. 1956).

Because the bankruptcy court in New York foreclosed the possibility of an evidentiary hearing, none was held. Nevertheless, the District Court improperly determined that it had sufficient grounds to grant the extraordinary relief of a preliminary injunction. That decision was in error because, as set forth above in the Statement of the Facts, the Court reached erroneous factual conclusions regarding a number of material fact issues. In light of the evidence in the record contradicting the Court's factual conclusions, the Court should not have issued injunctive relief without being able to conduct an evidentiary hearing. This was particularly true in light of the complex technology at issue in the case.

III. Appellees Failed to Establish a Likelihood of Success on the Merits

A. The Substantive Law of Contributory and Vicarious Infringement: *Sony* and its progeny.

In *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984), the

United States Supreme Court made clear that the judicially created doctrines of secondary copyright infringement must be applied with restraint, lest the doctrines allow the copyright holder improperly to extend his or her monopoly rights beyond the copyrighted work effectively to exert control over technologies or other matters not within the limited monopoly afforded by copyright law. In Part II of its Opinion, the Court emphasized that copyright law is not intended to benefit private interests, but rather to provide *just enough* incentive to authors to induce the release of creative works to the public. *Id.* at 429. Furthermore, achieving the proper balance so that the copyright holder's monopoly is not extended beyond the minimum scope necessary to effectuate that goal is a task properly left to Congress, not the Courts. *See id.* at 431; *accord Eldred v. Ashcroft*, 123 S. Ct. 769, 782 (2003) ("Calibrating rational economic incentives, however, like 'fashioning . . . new rules [in light of] new technology,' *Sony*, 464 U.S., at 431, is a task primarily for Congress, not the courts.").

In Part III of its Opinion, the Court turned its attention to the case at hand and the appropriate scope of the judicially created doctrines of contributory and vicarious copyright infringement. Owners of copyrighted television shows had sought to enjoin the distribution to the public of videotape recorders ("VTRs") – at the time a new technology – on the grounds that the distributors knew that the VTRs were being widely used to record copyrighted television shows without authorization. The Court first considered and rejected the copyright owners' argument "that supplying the 'means' to accomplish an infringing activity and

encouraging that activity through advertisement are sufficient to establish liability for copyright infringement." *Id.* at 436. Instead, the Court noted, "the label 'contributory infringement' has been applied in a number of lower court cases involving an ongoing relationship between the direct infringer and the contributory infringer at the time the infringement occurred. … [and in which] the `contributory' infringer was *in a position to control the use of copyrighted works by others and had authorized the use* without the permission of the copyright owner." *Id.* at 437 (emphasis added).

Because the situation before it did not fall into that category, the Supreme Court set out to determine whether there was any precedent for the copyright owners' requested relief. Copyright law provided no basis, so the Court turned to the Congressional enactments in patent law for guidance, and particularly the contributory infringement standard in 35 U.S.C. § 271(c). *Id.* at 435, 439-42. Under § 271(c),

> [t]he prohibition against contributory infringement is confined to the knowing sale of a component especially made for use in connection with a particular patent. . . . Moreover, the Act expressly provides that the sale of a "staple article or commodity of commerce suitable for substantial noninfringing use" is not contributory infringement.

Id. at 440. The reason for the limited scope of contributory liability, the Court explained, is that a

> finding of contributory infringement is normally the functional equivalent of holding that the disputed article is within the monopoly granted to the patentee.
>
> For that reason, in contributory infringement cases arising under the

> patent laws the Court has always recognized the critical importance of not allowing the patentee to extend his monopoly beyond the limits of his specific grant. These cases deny the patentee any right to control the distribution of unpatented articles unless they are "unsuited for any commercial noninfringing use." … "[A] sale of an article which though adapted to an infringing use is also adapted to other and lawful uses, is not enough to make the seller a contributory infringer. Such a rule would block the wheels of commerce."

Id. at 441 (citations omitted). The Court concluded:

> We recognize there are substantial differences between the patent and copyright laws. But in both areas the contributory infringement doctrine is grounded on the recognition that adequate protection of a monopoly may require the courts to look beyond actual duplication of a device or publication to the products or activities that make such duplication possible. The staple article of commerce doctrine must strike a balance between a copyright holder's legitimate demand for effective -- not merely symbolic -- protection of the statutory monopoly, and the rights of others freely to engage in substantially unrelated areas of commerce. Accordingly, the sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. *Indeed, it need merely be capable of substantial noninfringing uses*.

Id. at 442.

Courts of Appeal for other circuits have applied *Sony* to the distribution of software on at least two occasions. In one case, the Fifth Circuit found no contributory liability on the part of a software company that distributed a computer program designed to "facilitate the duplication of programs placed on copy-protected diskettes." *Vault Corporation v. Quaid Software Ltd.*, 847 F.2d 255, 258 (5th Cir. 1988). The court reached its conclusion after determining that the computer program had a single substantial noninfringing use – the creation of archival copies of the copy-protected diskettes. Accordingly, the Fifth Circuit held that the

"advertisement and sale" of the computer program by the defendant did not constitute contributory copyright infringement. *Id.* at 267.

More recently, the Ninth Circuit Court of Appeals applied *Sony* to claims of contributory and vicarious infringement through operation of a system that was somewhat similar to (though fundamentally different from) that of the Defendants here. In that case, *A&M Records v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001), Internet users with Napster's software could exchange files directly with one another without Napster acting as a conduit for the file transmission. Applying *Sony*, the court opined:

> 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 knows of and contributes to direct infringement. Conversely, 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. To enjoin simply because a computer network allows for infringing use would, in our opinion, violate *Sony* and potentially restrict activity unrelated to infringing use.

Id. at 1021 (citations omitted; emphasis added). With regard to vicarious liability, the court stated that while a system operator must police activity on its system to the extent of its right and ability to do so, that "'right and ability' is cabined by the system's current architecture." *Id.* at 1023. In other words, the fact that the system operator could fundamentally change the system's architecture in an effort to gain the ability to police the system does not mean that the operator has the requisite "right and ability" to police sufficient to impose vicarious liability. The Ninth Circuit ultimately concluded that Napster did have the requisite knowledge and

ability to control to establish contributory and vicarious liability. That conclusion, however, hinged upon the factual determination that Napster could locate infringing material in its indices, identify the purveyors of the infringing material, and terminate access to its system for those identified purveyors. *Id.* at 1021-22. As discussed above in the Statement of Facts, the same is not true in this case.

This Court appears to have had little occasion to consider the contributory infringement doctrine, much less in the little explored world of cyberspace. In a pre-*Sony* case, the Court upheld contributory copyright infringement liability in a case where a vendor knowingly sold items (likely non-staple articles of commerce) used to create unauthorized derivative works. *See Midway Mfg. Co. v. Artic International, Inc.*, 704 F.2d 1009, 1013 (7th Cir. 1985). The Court devoted virtually no discussion to the doctrine, however, mentioning it only twice in the opinion. *See id.* And while the Court has acknowledged the doctrine of vicarious copyright infringement on at least two occasions, in neither of these cases did the Court extend vicarious liability beyond its traditional areas *respondent superior* scope. *See Hard Rock Café Licensing Corporation v. Concession Services, Inc.*, 955 F.2d 1143, 1150 (7th Cir. 1992) (refusing to hold flea market owner/operator liable for vendor's infringement of plaintiff's trademark under the rules of vicarious liability applicable to copyright violations); *Dreamland Ball Room, Inc. v. Shapiro, Bernstein & Co.*, 36 F.2d 354, 355 (7th Cir. 1929) (holding dance hall proprietor liable for independent contractor's infringement where contractor's performance of copyrighted music in dance hall was conceded as infringing).

B. The Standard for Contributory Infringement Articulated and Applied by the District Court is Contrary to the Law Established by *Sony*.

In the section of its Opinion addressing contributory infringement liability, the District Court relied on the standard enunciated by the Second Circuit in *Gershwin Publishing Corp. v. Columbia Artists Mgt., Inc.*, as the test for contributory infringement liability: "[O]ne 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." 443 F.2d 1159, 1162 (2nd Cir. 1971); *see* Opinion at 20. The District Court did not, however, mention the standard described later in the *Sony* decision: "[T]he label 'contributory infringement' has been applied in a number of lower court cases involving an ongoing relationship between the direct infringer and the contributory infringer at the time the infringement occurred. …[and in which] the 'contributory' infringer was *in a position to control the use of copyrighted works by others and had authorized the use* without the permission of the copyright owner." *Sony,* 464 U.S. at 437 (emphasis added). In a more recent description of the contributory infringement doctrine, the Second Circuit has quoted the standard in *Sony*, rather than the language from *Gershwin*. *See Softel, Inc. v. Dragon Medical & Scientific Communications, Inc.*, 118 F.3d 955, 971 (2nd Cir. 1997) ("To establish contributory infringement, Softel was required to show that Hodge 'authorized the [infringing] use.'"). Without getting into the question of whether the *Gershwin* standard remains good law after *Sony*, suffice it to say that the standard articulated by the United States Supreme Court in *Sony* should not be ignored. Because the District

Court did not incorporate *Sony*'s standard for contributory infringement into its analysis and instead held *Sony* to be completely inapplicable here, the Court erred as a matter of law in its interpretation of that doctrine.

The District Court held *Sony* to be inapplicable because it felt that the decision was distinguishable on a number of grounds. First, the District Court held that, because the principal use of VTRs was found to be noninfringing in *Sony*, *Sony* only applies if a noninfringing use is *actually* the *principal* use of the article. (Opinion at 26.) Such a holding, however, is directly contrary to *Sony's* the specific holding that the article "need merely be capable of substantial noninfringing uses." *Sony*, 464 U.S. at 442 (emphasis added). The district court in *Napster* likewise engrafted an "actual use" requirement onto *Sony*, which the Ninth Circuit rejected on appeal. *Napster*, 239 F.3d at 1021 ("The district court improperly confined the use analysis to current uses, ignoring the system's capabilities.") Here, the Defendants offered a wide variety of noninfringing purposes to which the private instant messaging software could be put to use, the most obvious being instant messaging itself – a very common form of communication among Internet users. (First Deep Declaration at ¶¶ 16 – 23.)

Next, the District Court opined that "Aimster" is a "service" rather than an "article of commerce," thereby rendering *Sony* inapplicable. (Opinion at 26 – 27.) The "service" components the Court identified were "the provision of software, the maintenance of the Aimster system, and the continuing control of editorial content (i.e. Club Aimster)." *(Id.* at 27.) The only difference between the distribution of

software and VTRs is that software is, in certain respects, less tangible than a VTR. However, at least two federal Courts of Appeal have applied the *Sony* doctrine to software, *see Napster*, 239 F.3d at 1020 – 21; *Vault Corporation v. Quaid Software Ltd.*, 847 F.2d 255, 262-67 (5th Cir. 1988), and this Court has held that software is a "good" under Article 2 of the Uniform Commercial Code. *See Micro Data Base Systems, Inc. v. Dharma Systems, Inc.*, 148 F.3d 649, 654 (7th Cir. 1998). With regard to "maintenance of the Aimster system," it is unclear exactly what the District Court meant, but if it was referring to the maintenance of the Defendants' servers and other "backbone" infrastructure for the instant messaging to take place, there is simply nothing in the rationale of *Sony* that suggests that a copyright owner should be able to extend its monopoly to control the use of Internet infrastructure devices through claims of contributory infringement. *See Sony* 464 U.S. at 441 n. 21. Finally, the District Court's reference to "continuing control of editorial content (i.e. Club Aimster)" as a reason not to apply *Sony* to the instant messaging software is apparently based on the Court's confusion as to the relationship between Club Aimster and the completely separate messaging software. As discussed above, Club Aimster was an online magazine that did not interoperate with the messaging software or otherwise have any connection to the software apart from incorporating the word "Aimster" in its name. Moreover, even if there was some connection, it strains the rationale of *Sony* greatly to suggest that "continuing control of editorial content" on a webpage justifies placing a staple

article of commerce in the effective control of particular copyright owners. *See Sony* 464 U.S. at 441 n. 21.

The District Court next distinguished *Sony* on the grounds that *Sony* did not involve "the unauthorized and widespread *distribution* of infringing works," which the Court perceived to be present in this case. (Opinion at 27.) The Court seemed to limit its view of *Sony* to situations involving "private, home use" of copyrighted works, stating that "Defendants cannot successfully contend that Aimster involves merely private, home use." (Opinion at 27.) Again, however, *Sony* expressly holds that the use of an article of commerce "need merely be capable of substantial noninfringing uses." Nothing in the *Sony* opinion limits that statement to the particular facts of the case or otherwise suggests that an article "capable of substantial noninfringing uses" somehow falls outside the holding's scope depending on the nature of the purportedly infringing uses.

The next ground on which the District Court distinguished *Sony* was its adoption of a judicial gloss laid on top of *Sony* whereby *Sony* is rendered inapplicable if, according to the District Court, "the products at issue are specifically manufactured for infringing activity, even if those products have substantial noninfringing uses." (Opinion at 27.) The Court concluded, without any explanation or reference to the record, that "Aimster is a service specifically designed to aid the infringing activities of its users."[2] (*Id.*) The primary case cited

[2] The only evidence in the record regarding the design purpose of the Aimster system is set forth in the Declaration of John Deep In Opposition to Plaintiffs' Motion For A Preliminary Injunction, in which Mr. Deep explains that the system is an instant messaging system designed to allow users to select other users as "buddies" and communicate with such

by the District Court, *Cable/Home Comm. Corp. v. Network Productions, Inc.*, held *Sony* inapplicable because the defendant "utilized and advertised these devices primarily as infringement aids and not for legitimate, noninfringing purposes." 902 F.2d 829, 847 (11th Cir. 1990). Such a rule, however– at least as the District Court has applied it -- cannot be squared with *Sony*, which unambiguously holds that a device "need merely be capable of substantial noninfringing uses." *Sony*, 464 U.S. at 442. In support of its holding, the *Sony* court looked to contributory infringement in patent law, where:

> [u]nless a commodity "has no use except through practice of the patented method," the patentee has no right to claim that its distribution constitutes contributory infringement. "To form the basis for contributory infringement the item must almost be uniquely suited as a component of the patented invention."

Id. at 441 (citations omitted). Nowhere in *Sony* does the Supreme Court suggest that a staple article of commerce capable of substantial noninfringing uses falls outside the scope of the Court's holding merely because its primary intended use (or its design purpose as the District Court here opined) is for infringing purposes. Such a rule, if applied, would deprive the consuming public of the staple article of commerce and place that article effectively within a copyright holder's control – a result plainly not intended by the Supreme Court.[3]

"buddies" by exchanging privacy-protected, encrypted messages and attachments. (First Deep Decl., at ¶¶ 3 – 23.)

[3] The other case cited by the District Court, *A&M Records v. Abdallah*, was a district court decision that merely suggested as "arguabl[e]" the possible rule adopted here by the District Court. 948 F.Supp. 1449, 1456 (C.D. Cal. 1996).

Finally, the District Court factually distinguished *Sony* on the grounds that the trial court in that case found that Sony Corporation had not "influenced or encouraged" the making of unlawful copies. (Opinion at 27 – 28.) However, such a distinction, even if accurate, would not render *Sony* inapplicable. As stated above, the standard for contributory infringement enunciated in *Sony* was a general statement of the law, not a fact-specific holding for that particular case. And the rationale of *Sony* – that a copyright holder's monopoly rights should not extend to staple articles of commerce capable of substantial noninfringing uses -- does not support enjoining a staple article of commerce simply because someone has "influenced or encouraged" the article's use for an infringing purpose. Even if such influence or encouragement is sufficient somehow to give rise to secondary infringement liability, only the activities constituting the "influence and encouragement" properly may be enjoined. The staple article of commerce still has noninfringing uses, and it should not be placed in the effective control of the copyright holder merely because someone has encouraged its use for different purposes. One need only look – as did the *Sony* court -- to analogous principles in patent law to understand this point. Section 271(b) of the Patent Act provides that "[w]hoever actively induces infringement of a patent shall be liable as an infringer." 35 U.S.C. § 271(b). To prove inducement,

> [i]t must be established that the defendant possessed specific intent to encourage another's infringement and not merely that the defendant had knowledge of the acts alleged to constitute inducement. The plaintiff has the burden of showing that the alleged infringer's actions induced infringing acts and that he knew or should have known his actions would induce actual infringements.

Manville Sales Corp. v. Paramount Systems, Inc., 917 F.2d 544, 553 (Fed. Cir. 1990). While one may induce infringement through activities connected to the distribution of a staple article of commerce, it is not the case that all distribution of the same article of commerce constitutes infringement. *See E. I. Du Pont de Nemours & Co. v. Mallinckrodt, Inc.*, 654 F.Supp. 890, 909 (S.D. Ohio 1987), *aff'd,* 833 F.2d 1022 (Fed Cir. 1987) (holding that the sale of a product with one set of instructions for a particular purpose gave rise to inducement liability under § 271(b), while the same company's sale of the same product with a different set of instructions for a different purpose did not give rise to liability); *see also Sony,* 464 U.S. at 441 ("'[A] sale of an article which though adapted to an infringing use is also adapted to other and lawful uses, is not enough to make the seller a contributory infringer. Such a rule would block the wheels of commerce.' *Henry v. A. B. Dick Co.*, 224 U.S. 1, 48 (1912).").

C. The District Court Applied an Improper Standard to Impose Vicarious Liability for Copyright Infringement.

"One may be liable as a vicarious infringer . . . if the defendant has the right and ability to supervise the infringing activities as well as a direct financial interest in those activities." *F. E. L. Publications, Ltd. v. National Conference of Catholic Bishops*, 466 F. Supp. 1034, 1040 (N.D.Ill.1978) (citing *Shapiro, Bernstein & Co. v. H. L. Green & Co.*, 316 F.2d 304 (2d Cir. 1963) and *Gershwin Publishing Corporation v. Columbia Artists Management, Inc.*, 443 F.2d 1159 (2d Cir. 1971)).

Until recently, the doctrine of vicarious liability has not been extended beyond its traditional *respondeat superior* roots.[4] The District Court, however, applied the doctrine in an overly expansive manner to embrace a situation where no *respondeat superior* relationship even arguably existed. By doing so, Mr. Deep submits that the Court overstepped it bounds. *See Sony*, 464 U.S. at 431 ("The judiciary's reluctance to expand the protection afforded by the copyright without explicit guidance is a recurring theme.").

Here, the District Court concluded that the Defendants had the requisite "right and ability to supervise" for purposes of vicarious infringement because, according to the District Court, "[t]he fact that users must log in to the system in order to use it also demonstrates that Defendants know full well who their users are." (Opinion at 29.) That finding, coupled with the fact that Defendants' Terms of Service state that users transferring infringing material may have their access to the system terminated, was deemed by the district court to be sufficient to establish Defendants' "right and ability to supervise" their system for vicarious liability purposes. *Id.* As set forth above, however, the factual conclusion that the Defendants could adequately identify infringing users and police their activities notwithstanding the encryption functionality of the system is contrary to the evidence in the record. (First Deep Declaration at 8 – 12; Declaration of John A. Deep in Opposition to Plaintiffs' Proposed Preliminary Injunction Order, Oct. 17, 2002, at ¶¶ 7 – 9.) In particular, the District Court's finding that the sign-in page

[4] *See* Matt Jackson, *Copyright Law as Communications Policy: Convergence of Paradigms and Cultures: One Step Forward, Two Steps Back: An Historical Analysis of Copyright Liability*, 20 CARDOZO ARTS & ENT. L.J. 367, 392-93 (2002).

for Club Aimster was a "log in to the [instant messaging] system" was based on the Court's misunderstanding of the distinction between the Club Aimster website and the private messaging software. Indeed, because all user information for users of the messaging software was encrypted – including any "log-in" information for the messaging software itself, there is simply no way that the Defendants could have "known full well" who the users were or otherwise monitor or control user activity. (First Deep Declaration at 8 – 12; Declaration of John A. Deep in Opposition to Plaintiffs' Proposed Preliminary Injunction Order, Oct. 17, 2002, at ¶¶ 7 – 9.) As such, because the District Court's finding of "right and ability to control" rested on a demonstrably incorrect factual predicate, Mr. Deep submits that the Court erred.[5]

The district court also found that unspecified "infringing activities act[ed] as a draw for potential customers" and that Deep therefore had a direct financial interest in those infringing activities. (Opinion at 30.) Here, the court again misapplied the *Gershwin*/*F.E.L.* standard, resorting anew to swap meet jurisprudence to find a way to hold Deep liable. In *Gershwin*, the defendant, who admitted knowledge of the direct infringement, took a commission off the top from the fee paid the infringing performer for the infringing performance. *See Gershwin*, 443 F.2d at 1161. A more direct financial interest in infringing activity can hardly be imagined. Even in *Dreamland Ball Room*, where the dance hall proprietor

[5] The District Court also apparently rejected the Ninth Circuit's teaching that knowledge and ability to police are "cabined by the system's current architecture," *Napster*, 239 F.3d at 1023, holding that it was "disingenuous of Defendants to suggest that they lack the requisite level of knowledge when their putative ignorance is due entirely to an encryption scheme *that they themselves put in place*." (Opinion at 23; emphasis in original.) Mr. Deep likewise submits this aspect of the Court's holding to be erroneous.

conceded that the hired orchestra infringed, each person attending the infringing performance was charged a fee for admission to the performance. *See Dreamland Ball Room*, 36 F.2d at 355. In the instant case, users paid either nothing or a fixed monthly fee, which, since invariant, could in no way be directly related to any infringing activity. The district court therefore erred, since Deep did not have a direct financial interest in any infringing activity. Indeed, the very evidence that the court cites -- that Deep sold merchandise and solicited donations in conjunction with a web site -- militates for a finding that the financial interest of Deep were not tied to unspecified "infringing activities" but to the distinctiveness of Deep's product.

D. The District Court Failed to Properly Apply the Safe Harbor Provisions of the Digital Millennium Copyright Act.

In its opinion the District Court properly treated the Defendants as a "service provider" under the broad definition of that term set forth in the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 512(k)(1)(A). (Memorandum Opinion & Order at 34.) In addition, the district court found that the Defendants had adopted a "repeat infringer policy" as required by 17 U.S.C. § 512(i)(1)(A). (Memorandum Opinion & Order at 35.) However, the court held that subsection 512(i)(1)(A)'s terms were not met because the Defendants had not "reasonably implemented" that policy. (*Id.* at 36.) As such, the court found Defendants ineligible for the DMCA's safe harbor limitations on liability found in 17 U.S.C. § 512(a)-(d).

We submit that the District Court misapplied the "reasonably implemented" language in the DMCA. While the Court agreed that the Defendants could not

identify users of the private messaging software that were allegedly committing infringing acts, the Court held that obstacle to mean that the repeat offender policy was not being reasonably implemented. Specifically, the district court held, "[W]e remain nonplused with Defendants' arguments that the Aimster encryption system absolves them from responsibility when that scheme is voluntarily instituted by Defendants themselves. Adopting a repeat infringer policy and then purposefully eviscerating any hope that such a policy could ever be carried out is not an implementation as required by § 512(i)." (Memorandum Opinion & Order at 36 – 37.) In reaching that conclusion, the District Court erred in several respects. First, as discussed above in the Statement of Facts, the Court was plainly mistaken (and had no support in the record) in concluding that the policy was unenforceable. The policy could have been enforced to police the website forums and other non-encrypted portions of the websites; the fact that it could not easily be enforced against users of the private messaging software should not render the Defendants' efforts to implement the policy "unreasonable." Second, there simply is no support in the record for the court's factual conclusion that Defendants adopted its policy first and then designed an encryption system to eviscerate the policy. Finally, there exists no basis for the court's apparent legal conclusion that the safe harbors of the DMCA are not available to service providers having systems in which identification of infringing activity is difficult or impossible. There is nothing in the statutory language or legislative history of the statute to suggest such a construction, and the District Court's rule would substantially chill service providers' development and

use of any communications systems having encryption functionality. Indeed, the legislative history for a different portion of the DMCA – the anti-circumvention provisions enacted at 17 U.S.C. § 1201 – plainly reveals Congressional intent to promote private communications among individuals:

> In fact, enactment of section 1201 should have a positive impact on the protection of personal privacy on the Internet. The same technologies that copyright owners use to control access to and use of their works can and will be used to protect the personal privacy of Internet users by, for example, encrypting e-mail communications, or requiring a password for access to personal copyrighted information on an individual's web site. By outlawing the activities of those who make it their business to provide the tools for circumventing these protective technologies, this legislation will substantially enhance the degree to which individuals may protect their privacy as they work, play and communicate on the Internet.

Sen. Rep. No. 105-190 at p. 18 (1998).

We further submit that the District Court erred in its construction of the Transitory Communications Safe Harbor of the DMCA, set forth in 17 U.S.C. § 512(a). The District Court held section 512(a) to be inapplicable, reasoning that the private networks created by users were "peer-to-peer" networks and therefore "the information transferred between individual users does not pass 'through' Aimster's system at all." (Opinion at 37.) However, the plain language of section 512(a) does not require that the information pass through "Aimster" – it requires only that the information pass "through a . . . network controlled or operated by or for the service provider." Assuming *arguendo* that the District Court was correct that the Defendants somehow had sufficient knowledge and ability to police the private networks created by users of AbovePeer's private messaging software, then it

stands to reason that those networks were "controlled or operated" by the Defendants for purposes of section 512(a). As such, the District Court erred in its application of section 512(a).[6]

Finally, we submit that the District Court erred in its construction of the Information Location Tools Safe Harbor of the DMCA, 17 U.S.C. § 512(d). That subsection provides that a service provider will not be liable "by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link . . . ." *Id.* Because much of the District Court's holdings regarding contributory and vicarious liability are predicated on activities such as these (Opinion at 5 – 14, 20 - 30), the applicability of that safe harbor is important. The District Court concluded that the safe harbor is not available to Defendants because Defendants purportedly had knowledge of the infringing activity and had the right and ability to control the activity. (*Id.* at 40.) Such a construction of the DMCA's knowledge and right and ability to control elements – a construction similar to the district court's construction of the same elements for contributory and vicarious liability purposes – is erroneous in that *specific* knowledge of *specific* infringing activity should be the standard. The

[6] The District Court's secondary reason for finding section 512(a) inapplicable was the Court's erroneous factual conclusion in footnote 19 of its opinion that the materials did not pass through the network "without modification of its content" as required by the statute. In the District Court's view the encryption of transmissions using the private messaging software constituted a modification of the material. However, that encryption took place on the sender's computer before the material is sent, and any decryption took place at the other end on the recipient's computer. At no time were the encrypted transmissions modified while traveling through the private network.

statute provides that the safe harbor is not available for one who has actual or constructive knowledge of infringing materials or activity at "an online location." 17 U.S.C. § 512(d). The statute further provides that, upon receiving such knowledge, the service provider should "act[] expeditiously to remove, or disable access to, the material" in order to maintain the safe harbor protection. 17 U.S.C. § 512(d)(1)(C). In order for one to be able to "remove, or disable access to, the material," one obviously needs more than generalized knowledge of infringement is possibly taking place at some unidentified location on the Internet. Reading the subsections of the statute together, therefore, it is clear that Congress intended the actual or constructive knowledge of infringing materials or activity at "an online location" to be sufficiently specific that the online location itself can be identified, thereby allowing the service provider to take steps to remove or disable access to the material.

The District Court likewise rejected application of the Information Tools Safe Harbor on the ground that the Defendants "receive[d] a financial benefit directly attributable to the infringing activity [and] . . . ha[d] the right and ability to control such activity," which is a qualification to the safe harbor that removes its protections. That finding is incorrect for a number of reasons. First, as discussed above, the Defendants simply did not have the "right and ability to control" any allegedly infringing activity, and the District Court's conclusion that it did was based on confusion about the Defendants' ability to identify users by their log-in activities. Second, the legislative history to section 512 very plainly indicates that

the kind of financial benefit received here -- $4.95 each month for all users of Club Aimster – is not the kind of financial benefit contemplated by Congress. With regard to the identical language in section 512(c), the legislative history states:

> In general, a service provider conducting a legitimate business would not be considered to receive a ``financial benefit directly attributable to the infringing activity'' where the infringer makes the same kind of payment as non-infringing users of the provider's service.

H.R. Rept. 105-551, Part 2 at p. 54. Finally, the "right and ability to control" element should not foreclose the safe harbor to a service provider that provides encryption functionality to its users. In essence, the district court employed the same analysis for the DMCA that it used for contributory and vicarious liability – an approach that would virtually eliminate the safe harbor's availability for anyone otherwise liable for contributory or vicarious liability. *See* Charles S. Wright, *Actual Versus Legal Control: Reading Vicarious Liability For Copyright Infringement Into the Digital Millennium Copyright Act of 1998*, 75 WASH. L. REV. 1005 (2000). A "safe harbor" serves no purpose when it can be invoked only by those who can otherwise prove their innocence of the accused malfeasance.

IV. The District Court Failed to Properly Weigh the Irreparable Harm Occasioned Upon the Parties By the Grant or Denial of Injunctive Relief.

In determining whether to grant a preliminary injunction, a district court must not only consider the possible irreparable harm that may be suffered by the movant in the absence of an injunction, but also must weigh that harm against the irreparable harm that may be suffered by the non-movant if the injunction is granted. Here, the scale balancing irreparable harm tilts decidedly towards Mr.

Deep. The absence of a preliminary injunction would have, at best, negatively impacted the sales of various thriving corporations in a multi-billion dollar industry. The granting of a preliminary injunction, on the other hand, has destroyed a business and has taken the private messaging software provided by the Defendants completely off the market. *See Dos Santos v. Columbus-Cuneo-Cabrini Med. Cntr.*, 684 F.2d 1346, 1350-51 (7th Cir. 1982) (vacating preliminary injunction because it improperly deprived enjoined party of its entire business); *see also WarnerVision Entertainment Inc. v. Empire of Carolina*, 101 F.3d 259, 261-62 (2nd Cir. 1996) (upholding denial of preliminary injunction which, if granted, would have terminated enjoined party's rights).

V. The District Court Failed Adequately to Take into Account the Strong Public Interest At Stake.

As discussed above, the *Sony* decision reflects a strong public interest in having staple articles of commerce remain free of the control of copyright owners. By enjoining the distribution of software that can be used for a number of noninfringing purposes, the District Court's order extends the monopoly of certain copyright holders far beyond that necessary to promote the creation of original works.

VI. The Injunction Issued by the District Court is Unsupported by the Evidence, Overbroad in its Scope, and Impermissibly Vague.

Even if the District Court was correct to conclude that preliminary injunctive relief was necessary here, the actual injunction issued by the Court was legally deficient in a number of ways. After issuing its Opinion, the district court adopted,

almost *verbatim*, the preliminary injunction language tendered by the Appellees. The injunction begins by defining those subject to its strictures (collectively called "Aimster") in an astonishingly broad fashion:

> Defendants John A. Deep, AbovePeer, Inc., and Buddy USA, Inc. ("Defendants"), and their respective agents, servants, employees, representatives, subsidiaries, shareholders, officers, directors, principals, successors, assigns, licensees, transferees (including, without limitation, any purchasers, assigns, licensees, or transferees of any software or file-copying technology owned or controlled by Defendants), and all those acting in concert with them or at their direction or control (collectively "Aimster")

(Preliminary Injunction Order at 1).

In the following paragraph, the sweeping language of the injunction continued, this time with respect to the conduct it prohibited:

> 1. Aimster is preliminarily enjoined from directly, indirectly, contributorily, or vicariously infringing in any manner any and all sound recordings and musical compositions (or portions thereof) protected by federal or state law, whether now in existence or later created, in which Plaintiffs (and any parents, subsidiaries, or affiliates of Plaintiffs) own or control and exclusive right to reproduce, distribute, or transmit ("Plaintiffs' Copyrighted Works")."
>
> 2. Aimster shall immediately disable and prevent any and all access by any person or entity ("User") to any of Plaintiffs' Copyrighted Works available on, over, through, or via *any website, server, hardware, software, or any other system or service owned or controlled by Aimster (the "Aimster System and Service"), including, if necessary, preventing any and all access to the Aimster System and Service in its entirety*, until such time that Aimster implements measures that prevent any and all copying, downloading, distributing, uploading, linking to, or transmitting of Plaintiffs' Copyrighted Works on, over, through, or via the Aimster System and Service.

(Preliminary Injunction Order at ¶¶1- 2; emphasis added.)

The language of paragraph one merely parrots the language of the Copyright

Act in its prohibition against "infringing" the copyrights of Appellees, thus compelling Deep to make a legal judgment as to what conduct would be held to "infringe" Appellees' copyrights.

Paragraph two requires Mr. Deep to prevent any person that falls under the broad definition of "Aimster" from accessing, transferring, or copying any "Copyrighted Work" owned by Appellees through the use of any website, hardware or software owned or controlled by "Aimster." If Mr. Deep is unsuccessful, then he and the rest of the broadly defined "Aimster" must "prevent any and all access to the Aimster System and Service in its entirety." That means, for example, that if any former user of the private messaging software (all licensees of AbovePeer) somehow "accesses" any "Copyrighted Work" of Appellees (an undefined body of works) on his or her computer (which is considered part of the "Aimster System or Service"), then all of "Aimster" must shut down completely the "Aimster System and Service" (which includes all hardware and software owned or controlled the large group of people and companies comprising "Aimster"). Mr. Deep, being only one of many individuals comprising "Aimster" may not even turn on his computer (which, for a computer programmer, makes earning a livelihood rather difficult). Notably, the same most likely applies to the various individuals and companies/law firms that provided the many screen shots attached to Appellees' declarations tendered to the District Court. Those individuals and/or companies could only have obtained the screen shots by downloading the private messaging software at issue and agreeing to a license to use the software. That makes all of those people "licensees"

of AbovePeer and therefore members of the collective "Aimster."

A. The Injunction Was Issued Based Upon a False Premise: that Defendants Had or Could Obtain Knowledge of Which Users Are Engaged in Direct Copyright Infringement.

Contrary to the District Court's findings, there was no evidence to support the district court's conclusion that: 1) any users of the system had engaged in direct copyright infringement; and 2) the Defendants had specific knowledge of any direct infringement by the system's users, or that the Defendants were even *capable* of possessing such knowledge given the system's architecture. The District Court found, based on Appellees' declarations, that agents working on behalf of Appellees could use the system to make copies of copyrighted music, which conduct would have been an infringement in the absence of authorization from the copyright owners. From this premise, the Court mistakenly concluded that Appellees had provided evidence that *many, many other* users of the system were engaging in "massive" copyright infringement: This conclusion is contradicted by direct and unrefuted evidence regarding the encrypted nature of the communications, which prevents the Defendants, the Appellees, and the Court from ascertaining what materials are being transferred. Further, even if direct infringement were occurring, there is no evidence that Defendants could possibly prevent the alleged infringing activities from occurring in any manner other than possibly by removing the messaging software from the market and shutting off all infrastructure support.

B. The District Court Abused Its Discretion by Entering an Overly Broad Injunction.

The law is clear that, given the extraordinary nature of injunctive relief, any

injunction must be narrowly and appropriately tailored to the specific facts before the court. Accordingly, any injunction that exceeds those boundaries must be reversed as an abuse of discretion. *See, e.g.*, *E. & J. Gallo Winery v. Gallo Cattle Co.*, 967 F.2d 1280, 1297 (9th Cir. 1992).

i. The Injunction Enjoins Constitutionally-Protected Speech and Is Therefore An Impermissible Prior Restraint In Violation of the First Amendment.

The District Court's preliminary injunction enjoins the Defendants from any use of their computers, including use of those computers to conduct constitutionally protected speech, including the transfer of lawful computer software, source code, programming ideas and protocols, as well as protected political expression. Such an injunction constitutes a "prior restraint," *Chicago Council of Lawyers v. Bauer*, 522 F.2d 242, 248 (7th Cir. 1975), and therefore "[carries] a 'heavy presumption' against its constitutional validity." *Organization for a Better Austin v. Keefe*, 402 U.S. 415, 419 (1971). While an appropriately tailored injunction could have avoided this constitutional infirmity, the District Court's broad injunction prohibits a wide range of conduct that encompasses ordinary lawful activity, constitutionally-protected speech, as well as the allegedly infringing activity towards which the Appellees have directed this lawsuit.

ii. The Injunction Improperly Prohibits Conduct That Was Not at Issue Before It.

The District Court completely enjoined all use of Defendants' technology by precluding Defendants, any licensees of the technology, and any assigns of the

technology from operating it. (Preliminary Injunction Order at ¶¶ 1 – 2) Moreover, the court's order enjoins Defendants, their shareholders, licensees, assigns, *etc.* from any use of their computers whatsoever, and any use of the Internet whatsoever, regardless of whether such use has any remote connection to Appellees' charges of infringement, and without any determination as to the lawfulness of such activity as has been prohibited by the injunction. (*Id.*)

Such a broad injunction in the face of the narrow range of issues and facts before it is clearly impermissible:

> "Pursuant to 17 U.S.C. s 502, a permanent injunction may issue on such terms as the court deems "reasonable to prevent or restrain infringement of a copyright." This phrase has been interpreted to mean that a court's authority to issue an injunction in a copyright case should be limited in scope to that part of the work that is protectible."

Lipton v. Nature Co., 71 F.3d 464, 474-75 (2nd Cir. 1995) (citing 3 NIMMER ON COPYRIGHT s 14.06[C], at 14-109 ("The scope of the injunction therefore, should generally be no broader than the infringement, . . .); *see also Kepner-Tregoe, Inc. v. Leadership Software, Inc.*, 12 F.3d 527, 538 (5th Cir. 1994) (district court's injunction prohibiting defendant from modifying program at issue in future based on defendant's copyright infringement of current program is overbroad).

iii. Mr. Deep Can Only Comply with the Injunction by Shutting the System Down.

The evidence before the District Court established unequivocally that AbovePeer's private instant messaging software was "capable of substantial noninfringing uses." *Sony* requires no more. Given the extraordinarily broad scope of the injunction, the District Court effectively required Mr. Deep and the other

Defendants to cease doing business (at least any business that requires the use of computers). This was ordered notwithstanding the fact that the private messaging software was clearly capable of noninfringing uses. Thus the entry of this order was based on a fundamental misunderstanding of the law under *Sony*, improperly extended to prohibit perfectly legal activity, and hence is overbroad.

C. The Injunction is Impermissibly Vague.

Any injunction must be crafted with sufficient specificity so as to give notice to all those subject to it of the conduct that is prohibited thereby:

> "The judicial contempt power, even in its civil form, is a 'potent weapon,' *International Longshoremen's Ass'n v. Philadelphia Marine Trade Ass'n,* 389 U.S. 64, 76, 88 S.Ct. 201, 208, 19 L.Ed.2d 236 (1967), the use of which ought therefore to be confined to situations in which the defendant had clear notice that what he was doing violated a court order. That is why Rule 65(d) of the Federal Rules of Civil Procedure requires that injunctions be 'specific in terms' and 'describe in reasonable detail ... the act or acts sought to be restrained'; and it would not do to render general an injunction that was specific by free-wheeling interpretation of its terms."

Schering Corp. v. Illinois Antibiotics Co., 62 F.3d 903, 906 (7th Cir. 1995). The District Court's injunction is worded so broadly that a person seeking to determine its meaning is limited only by his or her imagination to determine what conduct might violate it.

i. The District Court Improperly Directed Defendants to "Not Violate the Law."

The very first paragraph of the District Court's injunction directed Defendants not to "directly, indirectly, contributorily, or vicariously infring[e]" the Copyrighted Works of Appellees. Because this language fails to give the enjoined party

reasonable notice of the conduct prohibited, courts have routinely condemned such language. See, e.g., *City of Mishawaka v. American Elec. Power Co.*, 616 F.2d 976, 991 (7th Cir.), *cert. denied*, 449 U.S. 1096 (1980) (vacating injunction that merely incorporated the broad language of the statute); *Ideal Toy Corp. v. Plawner Toy Mfg. Corp.,* 685 F.2d 78 (3rd Cir.1982) (injunction against "infringement" too vague);

The prohibition against the use of injunction language that prohibits the enjoined party from "violating the statute" or "infringing plaintiff's rights" is well-established in our jurisprudence. Indeed, the Supreme Court has explained that even if a party is found to been in violation of a statute,

> it does not follow that … the Board, in the circumstances of this case, is justified in making a blanket order restraining the employer from committing any act in violation of the statute, however unrelated it may be to those charged and found, or that courts are required for the indefinite future to give effect in contempt proceedings to an order of such breadth.. . . It would seem equally clear that the authority conferred on the Board to restrain the practice which it has found the employer to have committed *is not an authority to restrain generally all other unlawful practices which it has neither found to have been pursued not persuasively to be related to the proven unlawful conduct.*"

Nat'l Labor Rel. Bd. v. Express Publ. Co., 312 U.S. 426, 432-33 (1941) (emphasis added). In accordance with this principle, the Supreme Court explained:

> A federal court has broad power to restrain acts which are of the same type or class as unlawful acts which the court has found to have been committed or whose commission in the future unless enjoined, may fairly be anticipated from the defendant's conduct in the past. But the mere fact that a court has found that a defendant has committed an act in violation of a statute does not justify an injunction broadly to obey the statute and thus subject the defendant to contempt proceedings if he shall at any time in the future commit some new violation unlike and unrelated to that with which he was originally charged. This Court will strike from an injunction decree restraints

> upon the commission of unlawful acts which are thus dissociated from those which a defendant has committed.

Id. at 435-36 (citations omitted).

ii. The Injunction Order Improperly Placed Upon Defendants the Entire Burden of Identifying All of Appellees' Copyrighted Works, Both Now and In the Future.

The District Court's injunction order expressly required the Defendants to undertake both the initiative and the expense of identifying all of Appellees' Copyright Works, and to monitor the system to ensure that those works were not transferred using the system. Notwithstanding the technical impossibility of complying with that request given the encryption scheme in place, the District Court's order is flawed for a more fundamental legal reason: it is always the copyright holder's burden to identify the copyrighted works that are allegedly being infringed as a prerequisite to receiving the benefit of injunctive relief. *See A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1027 (9th Cir. 2001).

Conclusion

For the foregoing reasons, Appellant John Deep respectfully requests that the preliminary injunction entered by the District Court be vacated in its entirety.