

LONDON-SIRE RECORDS, INC., et al.

v.

DOE 1 et al.

UNITED STATES DISTRICT COURT FOR THE DISTRICT OF
MASSACHUSETTS

542 F. Supp. 2d 153 (2008)

GERTNER, D.J.:

ORDER ON MOTIONS TO QUASH

This case consists of numerous actions consolidated under London-Sire Records, Inc. v. Does 1-4, Civil Action No. 04-cv-12434. The plaintiffs include several of the country's largest record companies. The defendants, the plaintiffs claim, are individual computer users -- mainly college students -- who use "peer-to-peer" file-sharing software to download and disseminate music without paying for it, infringing the plaintiffs' copyrights.

1 The defendants in this case have not yet been named; the Court simply refers to them as "the defendants." Those who contest the subpoena are "the movants."

In these cases, the plaintiffs have been able to infer some infringing file-sharing activity from their investigations, but have not been able to discover the file-sharer's identity. They have an Internet Protocol [*158] number ("IP number" or "IP address") identifying the file-sharer's computer, but no more. Consequently, the plaintiffs [**4] -- with the Court's permission -- have served subpoenas on a number of internet service providers ("ISPs"), largely colleges and universities, seeking a name to go with the number. To preserve the rights of those whose identities are sought, the Court has required the ISPs to delay responding to the subpoena until the individual defendants have had an opportunity to move to quash it before their identities are disclosed.² Several defendants have done so; those are the motions presently before the Court.

2 Specifically, the Court requires that the plaintiffs attach a "Court-Directed Notice Regarding Issuance of Subpoena," which the ISPs distribute to the individuals in question. The Notice informs the putative defendants that they have the opportunity to move to quash the subpoena, as these defendants have done.

I. BACKGROUND

A. Facts

In each of these cases, the facts are substantially identical. Since the defendants' motions are effectively motions to dismiss -- there is almost no evidence in the case, and the movants argue, among other things, that the plaintiffs have failed to state a claim upon which relief can be

granted -- the Court will apply that standard of review to the pleadings. The plaintiffs' pleadings are taken as true, and the Court will draw all reasonable inferences in their favor. See, e.g., *Rivera v. Rhode Island*, 402 F.3d 27, 33 (1st Cir. 2005) (stating standard for motion to dismiss). To survive a motion to dismiss, the plaintiffs' pleaded facts must "possess enough heft to sho[w] that [they are] entitled to relief." *Clark v. Boscher*, 514 F.3d 107, 112 (1st Cir. 2008) (internal quotation marks omitted) (quoting *Bell Atlantic Corp. v. Twombly*, U.S. , 127 S. Ct. 1955, 1959, 167 L. Ed. 2d 929 (2007)) (first alteration in Twombly).

[*159] The plaintiffs allege that the defendants used peer-to-peer software to "download and/or distribute to the public certain of the [plaintiffs'] Copyrighted Recordings. . . . Through his or her continuous and ongoing acts of downloading **[**7]** and/or distributing to the public the Copyrighted Recordings, each Defendant has violated Plaintiffs' exclusive rights of reproduction and distribution." E.g., Compl. at 5 (docket no. 07-cv-10834, document # 1). To clarify the issues on which this case turns, the Court will briefly explain the nature of peer-to-peer software and its use.

Peer-to-peer software primarily exists to create decentralized networks of individual computer users. The software allows the users to communicate directly with one another, rather than routing their transmissions through a central server -- thus the term "peer-to-peer" architecture, as opposed to "client-server." See, e.g., *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913, 919-920, 125 S. Ct. 2764, 162 L. Ed. 2d 781 & n.1 (2005). Each type of architecture has distinct advantages and disadvantages, most of which are not relevant to this case.

What is relevant is that users in a peer-to-peer network can remain relatively anonymous or pseudonymous. Because communications between two computers on a peer-to-peer network can take place directly, without passing through a central network server,⁴ such transactions are not easily observable by a third party. By the nature **[**8]** of the network and software, then, peer-to-peer users can control what information they display to the world. See Linares Decl. at 4, Ex. A to Pl. Mot. Leave to Take Immediate Discovery (docket no. 07-cv-10834, document # 5). Moreover, generally speaking, anyone who has the requisite software and internet connection can participate in open peer-to-peer networks, such as the ones the defendants are alleged to have used in this case.

⁴ This is a small oversimplification. Many popular peer-to-peer networks use a "supernode" architecture. A supernode is a semi-centralized computer that operates only to relay search queries and responses within the peer-to-peer network. Once the desired file is located, however, it may be transferred directly from one computer to another. See, e.g., Peter S. Menell & David Nimmer, Legal Realism in Action: Indirect Copyright Liability's Continuing Tort Framework and Sony's De Facto Demise, 55 *UCLA L. Rev.* 143, 183-84 (2007).

The history of peer-to-peer networks has been one of increasing decentralization, and thus, increasing anonymity. See *id.* at 179-85 (tracing history of peer-to-peer network technologies through lawsuits asserting contributory copyright **[**9]** liability). Some newer peer-to-peer technologies even dispense with supernodes. See, e.g., *Grokster*, 545

U.S. at 922; Matthew Helton, Secondary Liability for Copyright Infringement: BitTorrent as a Vehicle for Establishing a New Copyright Definition for Staple Articles of Commerce, *40 Colum. J. L. & Soc. Probs. 1, 20-21 (2006)* (discussing new version of software that permits direct peer-to-peer connection without the need for a proxy computer).

Peer-to-peer users can also transfer files over the network. Many such files are entirely legitimate. See *Grokster*, *545 U.S. at 920*. However, other files transferred are electronic versions of copyrighted music or video files. Notably, because the files on each user's computer are digital, another computer can make a precise copy of them with no attendant loss in quality. See Linares Decl. at 3-4, Ex. A to Pl. Mot. Leave to Take Immediate Discovery (docket no. 07-cv-10834, document # 5).

In this case, the plaintiffs allege that each of the defendants has taken part in just such a file transfer. To discover potentially infringing transfers, the plaintiffs (acting through their trade association, the Recording Industry Association of America, [**10] or "RIAA") have retained a third-party investigator, MediaSentry, Inc. [*160] ("MediaSentry"). *Id.* at 4-5. MediaSentry essentially functions as an undercover user of the peer-to-peer networks. It connects to the network and searches for the plaintiff record companies' copyrighted files. Upon finding the files, it downloads them. See *id.* at 5-6. MediaSentry gathers what information it can about the computer from which the files were downloaded (the "sending computer.") Most crucially, that information includes the date and time at which the files were downloaded and the IP number of the sending computer. It can also include the user's name, but if given, the names are usually pseudonymous. See *id.* After the files are downloaded, the RIAA verifies that they can form the basis for a suit. It

reviews a listing of the music files that the user has offered for download in order to determine whether they appear to be copyrighted sound recordings. The RIAA also listens to the downloaded music files from these users in order to confirm that they are, indeed, illegal copies of sound recordings whose copyrights are owned by RIAA members.

Id. at 6. ⁵

5 At the hearing, the defendants protested that it is [**11] impossible to determine whether a sound recording is "illegal" merely by listening to it. See Bestavros Decl. at 2-3 (document # 110). True enough. Indeed, one of the key features of digital copyright infringement is that an nth-generation copy is more or less identical to a non-infringing first-generation copy, so there is no drop in sound quality over time. But listening to the files is still important. The defendants must ascertain that what is labeled as a sound recording to which they hold the copyright actually is such a recording [and not, say, a misnamed file or fair use that would not infringe the copyright.]

At this point, assuming the plaintiffs wish to sue, they cannot do so; they have only the IP number of the sending computer. An IP number is sometimes called an IP address because it is just that: an address. It serves as a locator declaring the place of a particular piece of electronic

equipment so that electronic data may be sent to it, and is usually represented as a series of four numbers between 0 and 255. See, e.g., *America Online v. Huang*, 106 F. Supp. 2d 848, 851 (E.D. Va. 2000). (For example, 168.122.128.38 is one of the IP addresses allegedly used by a defendant [**12] in this case. See Doe List, Ex. A to Compl. (docket no. 07-cv-10834, document # 1).)

But relatively few personal computer users have a specific, set IP address, called a "static" address. Instead, many use their computers to connect to a network provided by their ISP, which uses a certain range of IP addresses -- say, all of the numbers between 168.122.1.x to 168.122.100.x. The ISP assigns an address within its range to the user's computer for the user's session, allocating the numbers within its range on an as-needed basis. This process is known as "dynamic" addressing. See, e.g., H. Brian Holland, *Tempest in a Teapot or Tidal Wave? Cyber-squatting Rights & Remedies Run Amok*, 10 *J. Tech. L. & Pol'y* 301, 305 & nn. 13-18 (2005). This makes the plaintiffs' task of discovering the identity of a particular infringer more difficult. The IP address that they have noted as belonging to a particular user's computer may be assigned to a different user's computer in short order. See *id.*

However, the plaintiffs are not without leads. The range in which the IP address is assigned may reveal the user's ISP. See Linares Decl. at 7, Ex. A to Pl. Mot. Leave to Take Immediate Discovery (docket no. 07-cv-10834, [**13] document # 5); see also, e.g., Network-Tools.com, <http://network-tools.com/default.asp> (last visited Mar. 31, 2008) (providing such a service). And ISPs generally keep logs of which IP address is assigned to which user -- although it may purge those logs after a certain period of time, which was one of the key facts relied [*161] upon by the Court in granting expedited discovery. See Linares Decl. at 9, Ex. A to Pl. Mot. Leave to Take Immediate Discovery (docket no. 07-cv-10834, document # 5). Thus, the plaintiffs seek, through their subpoena, the opportunity to place their list of IP addresses side-by-side with the ISP's user logs to determine who was using the IP address at the moment of the alleged infringement. The ISPs, particularly colleges and universities, appropriately decline to reveal the identities of their users without a court order. Therefore, the plaintiffs bring "John Doe" lawsuits and seek discovery in order to determine the real identities of the defendants.

B. Procedural History

The plaintiff record companies have brought approximately forty "John Doe" cases in this Court, many -- perhaps most -- designating more than one defendant, grouped by ISP. In each case, the Court [**14] has granted expedited discovery and leave to subpoena the ISP, recognizing that the plaintiffs' rights may be irreparably and unfairly prejudiced unless they are allowed to seek the defendants' identities. See, e.g., Order re: Expedited Discovery (Dec. 9, 2004) (document # 7). Simultaneously, however, the Court has recognized that the defendants should have the opportunity to combat the subpoena if they desire to do so. Therefore, the Court has ordered that the ISP provide the individual users with notice of the lawsuit and a short statement of some of their rights before revealing their identities to the plaintiffs. Furthermore, the ISP may not respond to the subpoena for 14 days after each defendant has received notice. . . .

In view of the \$ 750 statutory minimum damages per song, 17 U.S.C. § 504(c)(2), most defendants choose to settle. The approximate settlement range appears to be \$ 3,000 to \$ 6,000 per

defendant, a considerable amount of money, particularly to the college students who have been caught in the plaintiffs' nets.

Only three of the defendants have elected to fight the subpoena. . . .

II. LEGAL STANDARDS

. . .

1. Whether the Plaintiffs [**26] Have Asserted a Claim Upon Which Relief Can Be Granted

A claim for copyright infringement has two elements. First, the plaintiffs must demonstrate that they hold a valid copyright (an issue the defendants do not contest.) Second, the plaintiff must show that the defendant violated one of the exclusive rights held by a copyright owner. . . . Two rights reserved to the copyright holder are at issue in this case: the right "to reproduce the copyrighted work in copies or phonorecords," *17 U.S.C. § 106(1)*, and the right "to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending," *id. § 106(3)*.

The movants and the amicus present two broad arguments, each of which requires [**27] the Court to consider the scope of a copyright holder's exclusive rights under the statutes quoted above. First, they contend that the copyright laws require an actual dissemination of copyrighted material; merely making copyrighted material available for another person to copy, they argue, is only an attempt at infringement -- which is not actionable. *Mem. Supp. Mot. Quash* at 4-6 (document # 104); *Mot. Quash* at 7 (document # 115); *EFF Br.* at 10-15 (document # 152). Second, they contend that the scope of the rights given to copyright owners by *§ 106* is limited by the definition of "phonorecords" as "material objects" in *17 U.S.C. § 101*.¹⁴ In their view, the copyright owner's rights are limited to tangible, physical objects, and purely electronic transmissions over the internet fall outside those rights.¹⁵ *Suppl. Mem. L. Supp. Mot. Quash* at 4-6 (document # 149); *Mot. Quash* at 7 (document # 115); *EFF Br.* at 15-24 (document # 152). Both of these broad arguments question whether the plaintiffs have alleged a legally cognizable [*166] harm under the copyright statutes. If they have not, then the subpoena must be quashed.

14 The parties refer to "copies." The statute makes clear that where sound [**28] recordings are at issue, "phonorecords" is a more precise term. See *17 U.S.C. § 101*. The two terms appear to be functionally interchangeable, however, differing only in the nature of the copyrighted work. . .

a. Whether the Copyright Holder's Right Extends Only to Actual Distributions

The first question the Court must address is whether the distribution right under *17 U.S.C. § 106(3)* requires an actual dissemination to constitute an infringement. It is an important issue, determining in part how to evaluate the proffered evidence in this case. MediaSentry, posing as just another peer-to-peer user, can easily verify that copyrighted material has [**29] been made available for download from a certain IP address. Arguably, though, MediaSentry's own downloads are not themselves copyright infringements because it is acting as an agent of the copyright

holder, and copyright holders cannot infringe their own rights. If that argument is accepted, MediaSentry's evidence cannot alone demonstrate an infringement.

The plaintiffs suggest two reasons why an actual distribution might not be required. First, the statute reserves to the copyright owner the right "to do and to authorize . . . [the distribution of] copies or phonorecords of the copyrighted work to the public." § 106(3) (emphasis added). The language appears to grant two distinct rights: "doing" and "authorizing" a distribution. Making the copyrighted material available over the internet might constitute an actionable "authorization" of a distribution. Second, if mere authorization is not enough, the plaintiffs argue that in appropriate circumstances -- including these -- "making available" copyrighted material is sufficient to constitute an act of actual distribution. Neither argument has merit.

The First Circuit has squarely considered and rejected the proposition that copyright liability arises where the defendant authorized an infringement, but **[**31]** no actual infringement occurred. See *Venegas-Hernandez v. Ass'n de Compositores & Editores de Musica Latinoamericana*, 424 F.3d 50, 57-58 (1st Cir. 2005). It noted that Congress' intent in adding "authorize" to the statute was to "avoid any questions as to the liability of contributory infringers." *Id.* at 58 (internal quotation marks omitted) (quoting H.R. Rep. 94-1476 ("House Report") at 52 (1976), reprinted in 1976 U.S.C.C.A.N. 5659, 5674). Authorization is sufficient to give rise to liability, but only if an infringing act occurs after the authorization. See *id.* at 59; see also *Latin Am. Music Co. v. The Archdiocese of San Juan of the Roman Catholic & Apostolic Church*, 499 F.3d 32, 46 (1st Cir. 2007) (citing and applying *Venegas-Hernandez*).

Thus, to constitute a violation of the distribution right under § 106(3), the defendants' actions must do more than "authorize" a distribution; they must actually "do" it. The Court therefore moves to **[*167]** the plaintiffs' second argument: Merely making copyrighted works available to the public is enough where, as in this case, the alleged distributor does not need to take any more affirmative steps before an unauthorized copy of the work changes hands. **[**32]** Other courts have split over whether that is a valid reading of the statute. Compare *Hotaling v. Church of Jesus Christ of Latter-Day Saints*, 118 F.3d 199 (4th Cir. 1997) (holding that making copyrighted material available is sufficient to constitute a distribution), and *Arista Records LLC v. Greubel*, 453 F.Supp.2d 961, 969-70 (N.D. Tex. 2006) (citing and following *Hotaling*), and *Warner Bros. Records, Inc. v. Payne*, No. W-06-CA-051, 2006 U.S. Dist. LEXIS 65765, 2006 WL 2844415, at *3-*4 (W.D. Tex. July 17, 2006) (same), with *In re Napster, Inc. Copyright Litig.*, 377 F. Supp. 2d 796, 802-05 (N.D. Cal. 2005) (criticizing *Hotaling* as being "contrary to the weight of [other] authorities" and "inconsistent with the text and legislative history of the Copyright Act of 1976"), and *Nat'l Car Rental Sys., Inc. v. Computer Assocs. Int'l, Inc.*, 991 F.2d 426, 434 (8th Cir. 1993) (stating that infringement of the distribution right requires the actual dissemination of copies or phonorecords).

To suggest that "making available" may be enough, the plaintiffs rely primarily on the Fourth Circuit's decision in *Hotaling*.¹⁸ In that case, a library had an unauthorized copy of a book, which it "made available" to the public; the **[**33]** defendant argued that without a showing that any member of the public actually read the book, it could not be liable for "distribution." See *id.* at

201-02, 203. The district court agreed and granted summary judgment to the defendant. The Fourth Circuit reversed:

When a public library adds a work to its collection, lists the work in its index or catalog system, and makes the work available to the borrowing or browsing public, it has completed all the steps necessary for distribution to the public. At that point, members of the public can visit the library and use the work. Were this not to be considered distribution within the meaning of § 106(3), a copyright holder would be prejudiced by a library that does not keep records of public use, and the library would unjustly profit by its own omission.

Id.; see also *id.* at 204.

The plaintiffs contend that this case is analogous to *Hotaling*, and suggest [*168] that the Court should reach the same conclusion as the Fourth Circuit. But [**35] the EFF correctly points out a lacuna in the Fourth Circuit's reasoning. See EFF Br. at 15 (citing William F. Patry, 4 Patry on Copyright §§ 13:9, 13:11 (2007)). Merely because the defendant has "completed all the steps necessary for distribution" does not necessarily mean that a distribution has actually occurred. It is a "distribution" that the statute plainly requires. See 17 U.S.C. § 106(3). . . .

But that does not mean that the plaintiffs' pleadings and evidence are insufficient. The Court can draw from the Complaint and the current record a reasonable inference in the plaintiffs' favor -- that where the defendant has completed all the necessary steps for a public distribution, a reasonable fact-finder may infer that the distribution actually took place. As in *Hotaling*, the defendants have completed the necessary steps for distribution, albeit electronic: Per the plaintiffs' pleadings, each individual Doe defendant connected to the peer-to-peer, network in such a way as to allow the public to make copies of the plaintiffs' copyrighted recordings. See Compl. at 5 (docket no. 07-cv-10834, document # 1). Through their investigator, the plaintiffs have produced evidence that the files were, in fact, available for [**40] download. They have also alleged that sound recordings are illegally copied on a large scale, supporting the inference that the defendants participated in the peer-to-peer network with the intent that other users could download from the defendants copies of the plaintiffs' copyrighted material. See Linares Decl. at 3-4, Ex. A to Pl. Mot. Leave to Take Immediate Discovery (docket no. 07-cv-10834, document # 5). At least at this stage of the proceedings, that is enough. The plaintiffs have pled an actual distribution and provided some concrete evidence to support their allegation. . . .

2. Whether the Plaintiffs Have Adduced Prima Facie Evidence of Infringement

. . . The movants and the EFF argue that because the plaintiffs have not demonstrated an actual [**60] infringement, they have not asserted an actual violation.³⁰ They reason that the [*176] investigator downloading the files from the defendants' computers was an agent of the plaintiffs, and plaintiffs cannot infringe their own copyrights. See Mem. Supp. Mot. Quash at 4-6 (document # 149); EFF Br. at 12 n.8 (document # 152).

The Court need not now decide the precise nature of the evidence MediaSentry gathered. While the parties dispute whether an investigator's download can be a perfected infringement, the downloads are also relevant, as described above, for another purpose: demonstrating that such infringement was technically feasible, thereby demonstrating that distributions could occur.

The plaintiffs have alleged that each defendant shared many, many music files -- at least 100, and sometimes almost 700. See Ex. A to Compl. (docket no. 07-cv-10834, document # 1) (providing information for each Doe, including number of copyrighted music files shared); Linares Decl. at 4, Ex. A to Pl. Mot. Leave to Take Immediate Discovery (docket no. 07-cv-10834, document # 5) (attesting to the veracity of the information [**62] contained in Exhibit A to the Complaint). As noted above, that evidence supports an inference that the defendants participated in the peer-to-peer network precisely to share copyrighted files. The evidence and allegations, taken together, are sufficient to allow a statistically reasonable inference that at least one copyrighted work was downloaded at least once. That is sufficient to make out a prima facie case for present purposes. Discovery may well reveal other factors relevant to the statistical inference, such as the length of time the defendant used peer-to-peer networks.

The plaintiffs have satisfied their burden for a prima facie case. As noted above, merely exposing music files to the internet is not copyright infringement. The defendants may still argue that they did not know that logging onto the peer-to-peer network would allow others to access these particular files, or contest the nature of the files, or present affirmative evidence rebutting the statistical inference that downloads occurred. But these are substantive defenses for a later stage. Plaintiffs need not prove knowledge or intent in order to make out a prima facie case of infringement. As noted above, they [**64] are not required to win their case in order to serve the defendants with process. . . .