

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

WEST BAY ONE, INC.

Plaintiff,

v.

DOES 1-2,000

Defendant.

CA. 1:10-cv-00481-RMU

**MEMORANDUM OF AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION,
PUBLIC CITIZEN, AMERICAN CIVIL LIBERTIES UNION FOUNDATION AND
AMERICAN CIVIL LIBERTIES UNION OF THE NATION'S CAPITAL IN SUPPORT
OF THIRD PARTY TIME WARNER CABLE'S MOTION TO QUASH OR MODIFY
SUBPOENA**

TABLE OF CONTENTS

INTRODUCTION.....1

STATEMENT OF INTEREST3

ARGUMENT5

I. The Court Appears to Lack Personal Jurisdiction Over the Vast Majority of the Defendants.....5

II. Plaintiff Has Improperly Joined Thousands of Individual Defendants Based on Entirely Disparate Alleged Acts10

III. The Court Must Balance the Right to Anonymous Speech Against the Need for Disclosure13

CONCLUSION19

INTRODUCTION

Amici file this brief because we are deeply concerned that serious problems of fairness, due process and individual justice are being raised by this and several related mass copyright lawsuits pending in this District against thousands of individual Internet users. In these cases different plaintiffs, represented by the same counsel, have sued thousands of anonymous, independent John Doe defendants from all over the country.¹ *Amici* have filed this brief in three of the cases, where Time Warner Cable (“TWC”) has moved to quash the subpoenas demanding the names of the individuals sued.²

The federal courts have safeguards, both procedural and substantive, to protect the rights of individual defendants and to ensure that each person sued has his or her defenses evaluated individually. Those safeguards apply in all litigation, regardless of the legal claims made. Certainly, copyright infringement is a legitimate basis for suit and if many people engage in copyright infringement, many people may be sued. But regardless of the legitimacy of the legal claims, the general safeguards developed by federal courts to ensure that all civil defendants get a fair chance to present their defenses should always apply.

Unfortunately, several of those safeguards have not been followed by the plaintiffs in these mass copyright cases, creating a situation that violates the legal rights of the John Doe defendants. In the instant case, almost all of the Doe defendants appear to be located outside this Court’s jurisdiction, and do not appear to have sufficient contacts with the District of Columbia to support being haled into court here. Further, Plaintiff has improperly joined thousands of

¹ As of June 2, 2010, strikingly similar Complaints had been filed in an additional four lawsuits. *Worldwide Film Entertainment LLC v. Does 1-749*, No. 1:10-cv-00038-HHK-DAR (D.D.C., filed Jan. 8, 2010); *G2 Productions LLC v. Does 1-83*, No. 1:10-cv-00041-CKK (D.D.C., filed Jan. 8, 2010); *Maverick Entertainment Group, Inc. v. Does 1-1000*, No. 1:10-cv-00569-RJL (D.D.C., filed April 8, 2010); *Voltage Pictures v. Does 1-5000*, No. 1:10-cv-00873-RMU (D.D.C. filed May 24, 2010). Time Warner Cable has not moved to quash in those cases, but *Amici* believe they present the same due process and First Amendment concerns raised herein.

² The three cases are *Achte/Neunte Boll Kino Beteiligungs GMBH & CO KG v. Does 1-4577*, No. 1:10-cv-00453-RMC (D.D.C., filed Mar. 18, 2010), *West Bay One v. Does 1-2000*, No. 1:10-cv-00481-RMC (filed Mar. 23, 2010) and *Call of the Wild Movie v. Does 1-358*, No. 1:10-cv-00455-RMU (D.D.C., filed Mar. 19, 2010).

unrelated Doe defendants in a single action, jeopardizing their right to an individual evaluation of their actions and defenses. Finally, Plaintiff has failed to identify the proper First Amendment protective legal test for the discovery the identity of persons who have communicated anonymously online, much less meet that test. As explained last year in *Sinclair v. TubeSockTedD*, 596 F. Supp. 2d 128 (D.D.C. 2009), individuals who communicate anonymously online may be identified only if a plaintiff meets a multi-factor test designed to balance the right to seek redress for legitimate claims against the fundamental right to communicate anonymously. Of particular importance here, before the defendant's identity can be disclosed, a plaintiff must come forward with some evidence that each individual defendant infringed the plaintiff's rights, and each defendant must be given notice and an opportunity to quash.

Amici are public interest organizations that have long been active in ensuring that court processes are fair to participants and comply with due process, including in similar mass copyright lawsuits brought by members of the Recording Industry Association of America ("RIAA") against sets of independent Doe defendants accused of unauthorized file-sharing of music ("the RIAA cases"). Several rulings in those cases, discussed more specifically below, rejected the precise tactics Plaintiff is using here. In others, most notably in the District Court for the Eastern District of Pennsylvania, courts set out specific procedures to ensure that individual Defendants would have a fair chance to defend themselves. *See Order, Elektra Entm't Group, Inc., et al. v. Does 1-6*, No. 04-1241 (E.D. Pa. Oct. 13, 2004) *Amici Curiae The Electronic Frontier Foundation, Public Citizen, American Civil Liberties Union Foundation And American Civil Liberties Union Of The Nation's Capital's Request For Judicial Notice In Support Of Motion To File As Amici Curiae In Support Of Third Party Time Warner Cable's Motion To Quash Or Modify* ("RJN") Ex. C and *In Re: Copyright Infringement Cases With Doe Defendants Related to Civil Action Number 04-1239*, Case No. 04-CV-650-CN, Dkt. 17 (E.D. Pa. January 21, 2005), RJN Ex. D.

Amici therefore respectfully urge this Court to grant TWC's motion to quash the subpoena issued to TWC, and to quash, sua sponte, the similar subpoenas issued to other ISPs in

this case. Additionally, we suggest that the Court instruct Plaintiff that any future subpoenas issued in this case to ISPs seeking the identity of anonymous Internet users must be accompanied by a cover notice ordering the ISP (1) to notify, within seven days of service of the subpoena, any person whose information has been sought that such information may be disclosed, and briefly describe their rights and options for protecting such information; and (2) to provide sufficient opportunity for the subscriber to exercise those rights, such as by moving to quash. Plaintiff may be required to compensate the ISP for additional costs, if any, associated with providing notice. To assist the Court, we attach hereto the standard procedures issued by the District Court for the Eastern District of Pennsylvania for the RIAA cases. *See* RJN Exs. C and D. Such procedures will help ensure that Plaintiff, Defendants, and the ISPs involved all have a fair opportunity to represent their interests.

Fed. R. Civ. P. 21 authorizes the Court to cure the improper joinder of parties by acting “on its own . . . at any time,” to “drop a party.” Accordingly, *Amici* further respectfully suggest that the Court cure Plaintiff’s improper joinder of the thousands of defendants named in this case by severing all but Defendant Doe 1 and “drop[ping]” Does 2 through 2000 from this action. Plaintiff may, of course, file new lawsuits in this District against any defendant, including Does 2-2000, as to whom Plaintiff can meet its burden of establishing jurisdiction.

STATEMENT OF INTEREST

The Electronic Frontier Foundation (“EFF”) is a non-profit, member-supported digital civil liberties organization. As part of its mission, EFF has served as counsel or *amicus* in key cases addressing user rights to free speech, privacy, and innovation as applied to the Internet and other new technologies, including several of the RIAA Cases discussed herein. With more than 14,000 dues-paying members, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age, and publishes a comprehensive archive of digital civil liberties information at one of the most linked-to web sites in the world, www.eff.org.

Public Citizen is a public interest organization based in Washington, D.C., which has

approximately 150,000 members and supporters. Since its founding in 1971, Public Citizen has urged citizens to speak out against abuses by a variety of large institutions, including corporations, government agencies, and unions, and it has advocated a variety of protections for the rights of consumers, citizens and employees to encourage them to do so. Along with its efforts to encourage public participation, Public Citizen has brought and defended numerous cases involving the First Amendment rights of citizens who participate in public debates. Public Citizen has been in the forefront of the development of the law to protect the right to speak anonymously on the Internet and to develop standards for determining when the right to speak anonymously should yield to a plaintiff's claimed right to identify a potential defendant in litigation. Public Citizen has represented Doe defendants or appeared as *amicus curiae* in numerous cases in which subpoenas have been sought to identify anonymous Internet users. *Mortgage Specialists v Implode-Explode Heavy Indus.*, __ A.2d __, 2010 WL 1791274 (NH May 6, 2010); *Independent Newspapers v. Brodie*, 966 A.2d 432 (Md. 2009); *Mobilisa v. Doe*, 170 P.3d 712 (Ariz. App. 2007); *Doe v. Cahill*, 884 A.2d 451 (Del. 2005); *Melvin v. Doe*, 836 A.2d 42 (Pa. 2003); *RIAA v. Verizon Internet Services*, 351 F.3d 1229 (D.C. Cir. 2003); *Dendrite Int'l v. Doe*, 775 A.2d 756 (N.J. App. 2001).

The American Civil Liberties Union (“ACLU”) is a nationwide, nonprofit, nonpartisan organization with over 500,000 members dedicated to the principles of liberty and equality embodied in the U.S. Constitution. The ACLU of the Nation’s Capital is the Washington, D.C. affiliate of the ACLU. The protection of principles of freedom of expression as guaranteed by the First Amendment is an area of special concern to the ACLU and its affiliates. In this connection, the ACLU and its affiliates have been at the forefront in numerous state and federal cases involving freedom of expression on the Internet. The ACLU and its affiliates have also been involved in numerous cases raising issues of due process and the right to engage in anonymous speech.

This case squarely impacts the interests of *Amici*’s members and the interests of anonymous Internet users. In this brief, *Amici* identify critical due process and First Amendment

requirements that must be taken into account before Plaintiff is permitted to intrude upon the rights of the anonymous Doe defendants.

ARGUMENT

I. The Court Appears to Lack Personal Jurisdiction Over the Vast Majority of the Defendants

This Court cannot consider this case unless it has personal jurisdiction over the Doe Defendants, and it is Plaintiff's burden to show that such jurisdiction exists. The Constitution imposes that burden on every plaintiff as a fundamental matter of fairness, recognizing that no defendant should be forced to have his rights and obligations determined in a jurisdiction with which he has had no contact. These requirements "give[] a degree of predictability to the legal system that allows potential defendants to structure their primary conduct with some minimum assurance as to where that conduct will and will not render them liable to suit." *World-Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286, 297 (1980).

Plaintiff has not met this burden. Instead, the very information upon which Plaintiff relies as a basis for seeking the identity of the Doe defendants – their Internet Protocol (IP) addresses – indicates that few, if any, reside in this District. If, as it appears, the vast majority of the Doe defendants do not have sufficient minimum contacts with this jurisdiction to satisfy due process, the Court should quash the subpoena for information about out-of-district defendants.

Identifying those home jurisdictions is no more difficult than identifying the ISP to which a given Defendant subscribes, something Plaintiff has already accomplished. As Plaintiff's declarant Patrick Achache admits, an IP address can provide "a general geographic area for the users." Declaration of Patrick Achache in Support of Plaintiff's Motion for Leave to Take Discovery Prior to Rule 26(f) Conference ("Achache Decl.") ¶ 12. As explained in the accompanying Declaration prepared by EFF Senior Staff Technologist Seth Schoen, many tools freely available to the public help reveal where a person using a particular IP address is likely to be physically located. *See* Decl. of Seth Schoen ("Schoen Decl.") ¶ 4. Two such techniques are reverse domain name service lookup or "reverse DNS" and access to the public database

operated by the American Registry for Internet Numbers (“ARIN database”). *See* Schoen Decl., ¶¶ 5, 13. Mr. Schoen used these tools both to confirm Plaintiff’s association of particular IP addresses with particular ISPs, and, more importantly to determine where Defendants are likely to be located. *See* Schoen Decl. ¶ 8-9. Focusing on IP addresses in Exhibit A to the Complaint that were associated with TWC’s RoadRunner service, Mr. Schoen concluded that the reverse DNS records indicated that the targeted TWC customers were likely located all over the country, from California to Florida, and that the same was true of Defendants who subscribed to other ISPs. *See* Schoen Decl. ¶ 10-12.

Thus, with minimal investigation, Plaintiff could have discovered that hardly any of the Does it has sued appear to reside in this District, *see* Schoen Decl. ¶18, and that therefore the case against them was likely not properly brought here. Nonetheless, Plaintiff improperly sued them here, apparently seeking to force almost all of the Doe defendants to incur the expense and burden of defense in a foreign District (or to settle in order to avoid that expense).

Moreover, Plaintiff provides no specific evidence other than its summary declarations to establish that its investigation was done for *each Doe*. And such evidence ought to be readily available, including screen shots showing the IP addresses of the Doe defendants so the Court can see that the addresses submitted to the Court match those discovered during the investigation, copies or real-time capture of the activities of the “proprietary technologies” used, and shots of the P2P server logs that to which Plaintiff apparently had access. Without those, the declarations merely describe downloading activity in general, and fail to provide the Court with real information linking each of the individuals sued to the alleged infringement.

Plaintiff attempts to get around this problem by asserting a sort of generalized Internet jurisdiction. Plaintiff claims that this Court has jurisdiction over these out-of-district individuals because (1) the alleged unlawful distribution took place over the Internet and, therefore “occurred in every jurisdiction in the United States, including this one”; and (2) each Defendant “contracted with an Internet Service Provider found in this District” for Internet access. Complaint ¶ 5.

On Plaintiff's theory, Internet users can be haled into court anywhere their ISP has significant contacts, or put another way, users can be haled into court anywhere their ISP has any other customers. This approach runs directly contrary to common sense and prevailing case law in this Circuit. In *GTE New Media Services Inc. v. BellSouth Corp.*, 199 F.3d 1343 (D.C. Cir. 2000), the Court of Appeals for the District of Columbia rejected a similarly expansive theory of jurisdiction. The plaintiff had argued that although the defendants had no physical contacts with the District of Columbia, they had "entered into an agreement outside of the District with an eye toward attracting Internet users in the District to their websites . . . and thereby draw advertisers away from [plaintiff]." *Id.* at 1349. The court noted that there was no evidence of financial harm to the plaintiff in the District of Columbia and squarely rejected the notion that the ability of a District of Columbia resident to access and use a website was sufficient to establish personal jurisdiction over the operator of the site:

When stripped to its core, GTE's theory of jurisdiction rests on the claim that, because the defendants have acted to maximize usage of their websites in the District, mere accessibility of the defendants' websites establishes the necessary "minimum contacts" with this forum. . . . This theory simply cannot hold water. Indeed, under this view, personal jurisdiction in Internet-related cases would almost always be found in any forum in the country. We do not believe that the advent of advanced technology, say, as with the Internet, should vitiate long-held and inviolate principles of federal court jurisdiction. The Due Process Clause exists, in part, to give "a degree of predictability to the legal system that allows potential defendants to structure their primary conduct with some minimum assurance as to where that conduct will and will not render them liable to suit." *World-Wide Volkswagen Corp.*, 444 U.S. at 297. In the context of the Internet, GTE's expansive theory of personal jurisdiction would shred these constitutional assurances out of practical existence. Our sister circuits have not accepted such an approach, and neither shall we.

Id. at 1350; *see also Sinclair*, 596 F. Supp. 2d at 133 (fact that defendants' statements posted on the Internet can be downloaded and viewed in the District of Columbia is insufficient to establish personal jurisdiction).

By contrast, the D.C. Circuit has found jurisdiction where, unlike here, the defendant had customers within the District of Columbia. In *Gorman v. Ameritrade Holding Corp.*, 293 F.3d 506, 511-13 (D.C. Cir. 2002), for example, the court had jurisdiction over defendant brokerage firm where D.C. residents could open brokerage accounts online and use them to buy and sell

securities, transmit funds, borrow and pay commissions and interest. Thus, the court noted, “[a]s a result of their electronic interactions, Ameritrade and its District of Columbia customers enter into binding contracts, the customers become owners of valuable securities, and Ameritrade obtains valuable revenue.” *Id.* at 512-13. In line with this precedent, in *Arista Records Inc. v. Sakfield Holding Co. S.L.*, 314 F. Supp. 2d 27, 31 (D.D.C. 2004), the court held that the evidence that a District of Columbia resident had subscribed to and used a music-downloading website, which required filling out personal information, agreeing to a license agreement, and downloading and installing proprietary software, was sufficient to establish personal jurisdiction over a nonresident website operator in a copyright infringement action brought by record companies.

These decisions are consistent with the general “sliding scale” rules for determining the proper jurisdiction for suits arising out of Internet activities. Under that case law, defendants who passively post information on the Internet for others to examine and copy are not subject to personal jurisdiction based on their Internet postings, while defendants whose Internet sites are commercially “interactive,” in the sense that they use their sites to engage in business transactions, are subject to being sued in any state in which a substantial number of business transactions occur. Along this continuum, the greater the degree of commercial interactivity, the greater the liability for suit in a foreign jurisdiction. *See, e.g., ALS Scan, Inc. v. Digital Serv. Consultants*, 293 F.3d 707, 714-15 (4th Cir. 2002) (no personal jurisdiction over nonresident ISP, in copyright infringement action brought by owner of photographs against ISP and its customer that allegedly published photographs on customer’s website, because ISP’s activities of providing bandwidth to the customer and publishing ISP’s own website were merely passive; ISP did not direct its electronic activity specifically at any target in district and did not manifest an intent to engage in a business or some other interaction in district); *Neogen Corp. v. Neo Gen Screening*, 282 F.3d 883, 888-89 (6th Cir. 2002) (finding personal jurisdiction where, in addition to other contacts, defendant not only maintained website but provided customers in the district with passwords so they could access confidential test results via that website); *Mink v. AAAA*

Dev. LLC, 190 F.3d 333, 336-37 (5th Cir. 1999) (maintenance of Internet website accessible to Texas consumers did not support exercise of personal jurisdiction over that defendant); *Cybersell, Inc. v. Cybersell, Inc.*, 130 F.3d 414, 419 (9th Cir. 1997) (no jurisdiction over a Florida corporation which had directed “no commercial activity over the Internet in Arizona. . . . [but only] post[ed] an essentially passive home page on the web ”).

The allegations against the Doe defendants in this case do not include claims of commercial interaction with anyone in the District of Columbia. At most, the thousands of Defendants here are accused of using a general software protocol to upload and download bits of copyrighted material via the Internet, a just as any passive website owner or participant in a message board discussion might. The mere possibility that someone in the District of Columbia might access data on a Doe’s computer is not a sufficient basis for subjecting that Doe to suit here, where he has done nothing to subject himself to this Court’s jurisdiction.

The fact that TWC provides service to *other people* in D.C. or is otherwise subject to jurisdiction here due to its own minimum contacts does not change the analysis with regard to the actual defendants in this lawsuit. Merely contracting with an ISP (or any other corporation) that happens to have other business in D.C. does not signify any intent of the customer to interact commercially with anyone in this District. TWC operates offices across the nation; the fact that it provides service in the District of Columbia cannot be the basis for suing its California or New York customers here. *See* Schoen Decl. ¶ 11 (Defendants appear to come from New York City, Southern California, Ohio, Florida and other states and regions). That conclusion would be equally obvious in other contexts; for example, a small Pennsylvania retailer who buys candy from Hershey does not thereby become subject to suit in Alaska because Hershey also sells candy to retailers in Alaska.

Requiring individuals from across the country to litigate in this District creates exactly the sort of hardship and unfairness that the personal jurisdiction requirements exist to prevent. It requires the individuals urgently to secure counsel far from home, where they are unlikely to have contacts. In this particular instance the hardship is very clear. When the underlying claim

is a single count of copyright infringement, the cost of securing counsel even to defend a defendant's identity is likely more than the cost of settlement, and possibly even more than the cost of judgment if the Defendant lost in the litigation entirely.

This is no theoretical concern. Already one Doe defendant in similar case (a Verizon subscriber), *Achte/Neunte*, No. 1:10-cv-00453-RMC, has stepped forward to assert her innocence, insisting she has never used the BitTorrent file-sharing protocol and has never heard of the movie she is alleged to have downloaded. *See* Nate Anderson, *Exclusive: "I've Never Heard of Far Cry," Says P2P Defendant*, Ars Technica, May 28, 2010, <http://arstechnica.com/tech-policy/news/2010/05/far-cry-innocence.ars>. In order to defend her innocence, however, she must quickly find counsel to help her understand rights and options, and also find the resources to pay that counsel. Before Plaintiff asks this Court to permit that burden to be imposed under its auspices, Plaintiff should meet *its* burden of showing this Court has jurisdiction over that Doe and every other Doe defendant.

Plaintiff's view essentially would allow general jurisdiction in any federal court against any person across the country, or even the world, so long as the claim involved Internet use, and based on no more evidence than a summary declaration describing a general investigative process. As explained above, federal courts have rejected this type of approach, and have instead required some affirmative, commercial interaction with people in the relevant district before jurisdiction may be exercised. The attempt should be rejected here as well.

II. Plaintiff Has Improperly Joined Thousands of Individual Defendants Based on Entirely Disparate Alleged Acts

There is little doubt that Plaintiff's joinder of two thousand Doe defendants in this single action is improper and runs the tremendous risk of creating unfairness and denying individual justice to those sued. Mass joinder of individuals has been disapproved by federal courts in both the RIAA cases and elsewhere. As one court noted:

Comcast subscriber John Doe 1 could be an innocent parent whose internet access was abused by her minor child, while John Doe 2 might share a computer with a roommate who infringed Plaintiffs' works. John Does 3 through 203 could be thieves, just as Plaintiffs believe, inexcusably pilfering Plaintiffs' property and

depriving them, and their artists, of the royalties they are rightly owed. . . . Wholesale litigation of these claims is inappropriate, at least with respect to a vast majority (if not all) of Defendants.

BMG Music v. Does 1-203, No. Civ.A. 04-650, 2004 WL 953888, at *1 (E.D. Pa. Apr. 2, 2004) (severing lawsuit involving 203 defendants).

Rule 20 requires that, for parties to be joined in the same lawsuit, the claims against them must arise from a single transaction or a series of closely related transactions. Specifically:

Persons . . . may be joined in one action as defendants if: (A) any right to relief is asserted against them jointly, severally or in the alternative with respect to or arising out of the same transaction, occurrence, or series of transactions or occurrences; and (B) any question of law or fact common to all defendants will arise in the action.

Fed. R. Civ. P. 20. Thus, multiple defendants may be joined in a single lawsuit only when three conditions are met: (1) the right to relief must be “asserted against them jointly, severally or in the alternative”; (2) the claim must “aris[e] out of the same transaction, occurrence, or series of transactions or occurrences”; **and** (3) there must be a common question of fact or law common to all the defendants. *Id.*

Joinder based on separate but similar behavior by individuals allegedly using the Internet to commit copyright infringement has been rejected by courts across the country. In *LaFace Records, LLC v. Does 1-38*, No. 5:07-CV-298-BR, 2008 WL 544992 (E.D.N.C. Feb. 27, 2008), the court ordered severance of lawsuit against thirty-eight defendants where each defendant used the same ISP as well as some of the same peer-to-peer (“P2P”) networks to commit the exact same violation of the law in exactly the same way. The court explained: “[M]erely committing the same type of violation in the same way does not link defendants together for purposes of joinder.” *LaFace Records*, 2008 WL 544992, at *2. In *BMG Music v. Does 1-4*, No. 3:06-cv-01579-MHP, 2006 U.S. Dist. LEXIS 53237, at *5-6 (N.D. Cal. July 31, 2006), the court *sua sponte* severed multiple defendants in action where the only connection between them was allegation they used same ISP to conduct copyright infringement. *See also Interscope Records v. Does 1-25*, No. 6:04-cv-197-Orl-22DAB, 2004 U.S. Dist. LEXIS 27782 (M.D. Fla. Apr. 1, 2004) (magistrate recommended *sua sponte* severance of multiple defendants in action where only

connection between them was allegation they used same ISP and P2P network to conduct copyright infringement); *BMG Music v. Does 1-203*, No. Civ.A. 04-650, 2004 WL 953888, at *1 (E.D. Pa. Apr. 2, 2004) (severing lawsuit involving 203 defendants); General Order, *In re Cases Filed by Recording Companies*, filed in *Fonovisa, Inc. et al. v. Does 1-41* (No. A-04-CA-550 LY), *Atlantic Recording Corporation, et al. v. Does 1-151* (No. A-04-CA-636 SS), *Elektra Entertainment Group, Inc. et al. v. Does 1-11* (No. A-04-CA-703 LY); and *UMG Recordings, Inc., et al. v. Does 1-51* (No. A-04-CA-704 LY) (W.D. Tex. Nov. 17, 2004), RJN Ex. A, (dismissing without prejudice all but first defendant in each of four lawsuits against a total of 254 defendants accused of unauthorized music file-sharing); Order Granting in Part and Denying in Part Plaintiffs' Miscellaneous Administrative Request for Leave to Take Discovery Prior to Rule 26 Conference, *Twentieth Century Fox Film Corp., et al., v. Does 1-12*, No. C-04-04862 (N.D. Cal Nov. 16, 2004) (in copyright infringement action against twelve defendants, permitting discovery as to first Doe defendant but staying case as to remaining Does until plaintiff could demonstrate proper joinder), RJN Ex. B.³

Courts in this District have embraced the same joinder principles. In *In re Vitamins Antitrust Litig.*, No. MISC 99-197 (TFH), 2000 WL 1475705, at *18 (D.D.C. May 9, 2000), for example, joinder was allowed when each of the defendants was alleged to be engaged in a single global antitrust conspiracy. But there is no allegation that the thousands of defendants in this action even know each other, much less that they engaged in a conspiracy. Nor does the allegation of a similar method for committing the alleged illegal activity create a basis for joinder. In *Nassau County Ass'n of Ins. Agents, Inc., v. Aetna Life & Cas. Co.*, 497 F.2d 1151 (2d Cir. 1974), for example, the Second Circuit refused to allow 164 insurance companies to be joined in a single action just because they allegedly used the same methods to cheat agents,

³ *Amici* recognize the judicial analysis was not universal. See, e.g., Order, *Motown Records v. Does 1-252*, No. 1:04-CV-439-WBH (N.D.Ga. Aug. 16, 2004) (denying motion to quash); Order, *Virgin Records Am. v. Does 1-44*, No. 1:04-CV-0438-CC (N.D.Ga. 2004, Mar. 3, 2004) (granting leave to take expedited discovery); *Sony Music Entm't, Inc. v. Does 1-40*, 326 F. Supp. 2d 556, 564 (S.D.N.Y. 2004) (applying First Amendment balancing test but denying as premature motion to quash as to misjoinder and lack of personal jurisdiction).

describing that attempted joinder as “a gross abuse of procedure.” *Id.* at 1154.

Plaintiff may argue that, unlike the RIAA cases, its allegations here are based upon use of the Internet to infringe a single movie. While that accurately describes the facts alleged in this case, it does not change the legal analysis. Whether the alleged infringement concerns a single copyrighted work or many, it was committed by unrelated defendants, at different times and locations, sometimes using different services, and perhaps subject to different defenses. That attenuated relationship is not sufficient for joinder. *See BMG Music v. Does 1-203*, 2004 WL 953888, at *1.

Nor does the analysis change because the BitTorrent protocol works by taking small fragments of a work from multiple people in order to assemble a copy. The individual Defendants still have no knowledge of each other, nor do they control how the protocol works, and Plaintiff has made no allegation that any copy of the movie they downloaded came jointly from any of the Doe defendants.

Joining thousands of unrelated defendants in one lawsuit may make litigation less expensive for Plaintiff by enabling it to avoid the separate filing fees required for individual cases and by enabling its counsel to avoid travel, but that does not mean these well-established joinder principles need not be followed here.⁴ Because this improper joining of these thousands of Doe defendants into this one lawsuit raises serious questions of individual fairness and individual justice, the Court should sever the defendants and “drop” Does 2-2000 from the case. *See Fed. R. Civ. P. 21.*

III. The Court Must Balance the Right to Anonymous Speech Against the Need for Disclosure

Plaintiffs are often allowed discovery at the outset of a lawsuit to identify otherwise unknown persons alleged to have committed a legal wrong. However, in its motion seeking

⁴ Several courts which have considered joinder have also noted that by filing a single lawsuit, the plaintiffs have avoided paying multiple filing fees. *See, e.g.,* General Order, *In Re: Cases Filed by Recording Companies*, RJN Ex. A, (ordering severance of 254 defendants sued in four cases before it, and noting that: “[t]he filing fees for the recent four cases totaled \$600, whereas the filing fees for 254 separate cases would have been \$38,100.”).

early discovery, (Dkt. No. 3), Plaintiff failed properly to apprise the Court of the appropriate procedure for seeking disclosure where, as here, Defendants were engaging in anonymous communication and Plaintiff's claims arise from those activities. Given the number of Doe defendants affected, both in this case and the numerous similar suits that have lately been filed in this District, it is crucial that the Court apply the correct procedure here and set an example of what appropriate procedures must be followed before individuals' identities can be disclosed.

Robust protection for the right to engage in anonymous communication – to speak, read, view, listen, and/or associate anonymously – is fundamental to a free society. *See, e.g., Talley v. California*, 362 U.S. 60 (1960) (recognizing the First Amendment right to communicate anonymously); *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 357 (1995) (same; “Anonymity is a shield from the tyranny of the majority.”); *Lamont v. Postmaster General*, 381 U.S. 301 (1965) (recognizing the First Amendment right to receive ideas in privacy). This fundamental right enjoys the same protections whether the context for speech and association is an anonymous political leaflet, an Internet message board or a video-sharing site. *See Reno v. ACLU*, 521 U.S. 844, 870 (1997) (there is “no basis for qualifying the level of First Amendment scrutiny that should be applied to” the Internet).

Courts in this District have recognized that First Amendment protections extend to the anonymous publication of expressive works on the Internet even where, as here, that publication is alleged to infringe copyrights. *In re Verizon Internet Servs. Inc.*, 257 F. Supp. 2d 244, 260 (D.D.C.), *rev'd on other grounds*, 351 F.3d 1229 (D.C. Cir. 2003) (hereinafter “Verizon”); *see also UMG Recordings, Inc., v. Does*, No. 06-0652 SBA, 2006 WL 1343597, at *2 (N.D. Ca. March 6, 2006) (citing *Sony Music Entm't, Inc. v. Does I-40*, 326 F. Supp. 2d 556, 564 (S.D.N.Y. 2004)). As the court in *Sony* noted:

Arguably, however, a file sharer is making a statement by downloading and making available to others copyrighted music without charge and without license to do so. Alternatively, the file sharer may be expressing himself or herself through the music selected and made available to others. Although this is not “political expression” entitled to the “broadest protection” of the First Amendment, the file sharer's speech is still entitled to “some level of First Amendment protection.”

326 F. Supp. 2d at 564 (quoting *Verizon*) (citations omitted). The *Sony* court continued:

“Against the backdrop of First Amendment protection for anonymous speech, courts have held that civil subpoenas seeking information regarding anonymous individuals raise First Amendment concerns.” *Id.* at 563.

Thus, the qualified privilege to speak or view information anonymously applies to the individuals whose identities are sought by these subpoenas. At the same time that the Court must consider the First Amendment rights at issue, however, it must also consider Plaintiff’s countervailing right to seek redress in a court of law and its need to identify anonymous Internet users in order to do so. As discussed below, federal and state courts performing this balancing have recognized that, at the outset of the litigation, the plaintiff has done no more than allege wrongdoing, and mere allegations generally do not overcome a privilege. They have further recognized that a serious chilling effect on anonymous speech would result if Internet users knew they could be identified by persons who merely allege wrongdoing, without necessarily having any evidence thereof, or any intention of carrying through with actual litigation.

Although Plaintiff barely acknowledged the First Amendment issues raised by its motion for leave to take early discovery, it did point to *Columbia Ins. Co. v. seescandy.com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999), one of the first cases to recognize this very tension, as the appropriate standard for evaluating disclosure of identifying information of Internet users. However, *Columbia v. seescandy.com* is no longer the leading case even in the Northern District of California, where it originated. See generally *Highfields Capital Mgmt, L.P. v. Doe*, 385 F. Supp. 2d 969 (N.D. Cal. 2005)

More appropriate guidance for the District of Columbia can be found in *Sinclair*, a defamation case in which the plaintiff sought disclosure of identifying information for a pseudonymous defendant. *Sinclair*, 596 F. Supp. 2d at 128. As explained in that case, two similar standards have emerged for identification of persons engaged in anonymous communication online. *Id.* at 132. The first is the five-part balancing test originally articulated in *Dendrite International v. Doe*, 775 A.2d 756, 760-61 (N.J. Super. Ct. App. Div. 2001), which

requires “(1) that the plaintiff undertake to notify the anonymous posters that they are the subject of a subpoena seeking their identity; (2) that the plaintiff specify the exact statement alleged to constitute actionable speech; (3) that the court review the complaint and other information to determine whether a viable claim against the anonymous defendants is presented; (4) that the plaintiff produce sufficient evidence to support, prima facie, each element of its cause of action; and (5) that the court then balance the First Amendment right of anonymous speech against the strength of the plaintiff's prima facie claim and the need for disclosure of the anonymous defendant's identity.” *Sinclair*, 596 F. Supp. 2d at 132. The second test “foregoes an explicit balancing of interests but still requires the plaintiff to come forward with sufficient evidence to establish a prima facie case on all elements of a claim that are supportable without discovery.” *Id.* (collecting cases). The *Sinclair* court declined to choose between the two, finding that the plaintiff's claims would fail under either test. *Id.* at 134.

The *Dendrite* test, particularly the explicit requirement that courts balance the parties' respective interests, is the appropriate test here. It has not been met.

First, Plaintiff has not demonstrated that it has made reasonable efforts to ensure that the Doe defendants have been notified that their identities are being sought. Plaintiff has not sought, and the Court's April 13, 2010 Order (Dkt. No. 4) granting leave to take discovery does not provide, sufficient procedures to ensure that Defendants are notified of the subpoenas for their identities and have a reasonable opportunity to obtain counsel and file a motion to quash.

Second, because this is a copyright action rather than a defamation action, it seems appropriate that, rather than being required to specify a defendant's exact statements, the plaintiff should be able to specify the nature and facts of the investigation leading to the charge of infringement against each defendant, to extent that the information is available prior to discovery. Plaintiff has access to a great deal of information prior to discovery -- such as the time, the nature and, to some extent, the physical location of the infringement -- so the threshold for a prima facie case should not be difficult to meet. Plaintiff may be able to meet this standard, but it has not yet done so. The First Amendment requires more information than has been

presented to the Court so far.

As to the fourth prong, Plaintiff's evidentiary showing here is thin. As noted above, Plaintiff merely submitted summary declarations, describing in general the steps taken by a British company to download and view the subject film. *See supra* at p. 6. Plaintiff has provided no specific evidence other than its summary declarations to support that these activities were done for each Doe defendant, although such evidence ought to be readily available and presentable to the Court in the form of screen shots or other printed pages documenting the investigation as to each Doe.

Plaintiff seeks to avoid meeting the First Amendment test by asserting that the Defendants have abandoned their right to speak anonymously by voluntarily providing identifying information to their service providers. That is not the rule. If it were, then *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449 (1958), and *Bates v. City of Little Rock*, 361 U.S. 516 (1960), were both wrongly decided. In those cases, the Supreme Court overturned penalties imposed on the NAACP and its officers for refusing to comply with orders to identify members, whose names the NAACP of course knew, on the ground that compelled identification violated the members' right to remain anonymous. Similarly, *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995) and *Talley v. California*, 362 U.S. 60 (1960), would have been wrongly decided because the authors of the unsigned leaflets identified themselves to their printers, and the distributors revealed their faces to the persons to whom they handed the leaflets. And, of course, *Sinclair, Dendrite*, and the many other decisions around the country applying the First Amendment balancing tests to disclosure of identifying information would similarly be incorrect under Plaintiff's view. *See, e.g., Best Western Int'l. v. Doe*, 2006 WL 2091695 (D. Ariz. July 25, 2006); *Highfields Capital Mgmt, L.P. v. Doe*, 385 F. Supp. 2d 969 (N.D.Cal., 2005); *Doe v. 2theMart.com, Inc.*, 140 F. Supp. 2d 1088, 1092 (W.D. Wash. 2001).

Indeed, since the identity of every speaker who has access to the Internet is known to his or her Internet Service Provider, either directly or through an intermediary (such as an employer) whose identity is known, such a rule would eviscerate the right to speak anonymously online.

See Sony Music Entm't, Inc., 326 F. Supp. 2d at 562 (“[t]he Internet is a particularly effective forum for the dissemination of anonymous speech”); *Doe v. 2theMart.com, Inc.*, 140 F. Supp. 2d 1088, 1092 (W.D. Wash. 2001) (“[t]he right to speak anonymously extends to speech via the Internet. Internet anonymity facilitates the rich, diverse, and far ranging exchange of ideas”); *Columbia Ins. Co.*, 185 F.R.D. at 578 (N.D. Cal. 1999) (“[t]his ability to speak one’s mind without the burden of the other party knowing all the facts about one’s identity can foster open communication and robust debate”).

Rather than address the First Amendment case law, Plaintiff incorrectly attempts to rely on Fourth Amendment jurisprudence. But the Fourth Amendment’s “reasonable expectation of privacy” standard for governmental searches is inapplicable where a plaintiff in a civil case seeks to overcome the more stringent protections for anonymous speech under the First Amendment. As a result, Plaintiff’s reliance on those cases is misplaced, including *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979); *Couch v. U.S.*, 409 U.S. 322, 335-36 (1973); *Guest v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001); *U.S. v. Kennedy*, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (no Fourth Amendment privacy interest in subscriber information produced to government investigators); *U.S. v. Hambrick*, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999). Furthermore, none of the Fourth Amendment cases Plaintiff cites holds that information held by third party communications providers may be freely disclosed without appropriate legal process. Disclosure of the subscriber information in *Guest*, *Kennedy*, and *Hambrick*, the pen register data in *Smith*, and the tax records in *Couch* was regulated by federal statute including the Electronic Communications Privacy Act, 18 U.S.C. § 2701 *et seq.*, the Pen Register Statute, 18 U.S.C. § 3121 *et seq.* and the tax code, 26 U.S.C. § 7602.

In the First Amendment context, even when the claim against a user is that he or she infringed copyrights, the First Amendment tests must be applied. *See, e.g., Arista Records LLC v. Doe 3*, No. 09-0905-cv, 2010 WL 1729107, at *7 (2d Cir. Apr. 29, 2010); *Interscope Records v. Does 1-14*, 558 F. Supp. 2d 1176, 1179-80 (D. Kan. 2008); *Sony*, 326 F. Supp. 2d at 565-67. The Court should hold Plaintiff to those stringent standards. Moreover, if it does determine that

Plaintiff has met the appropriate balancing test, the Court should, at a minimum, require ISPs to forward a copy of any subpoena seeking identifying information to the subpoena target within seven days, along with information outlining the target's legal options, and delay any disclosure so that he has an opportunity to protect his identity. As noted, elements of this procedure were included in Orders authorizing discovery issued by the District Court for the Eastern District of Pennsylvania in connection with the mass RIAA lawsuits. Order, *Elektra Entm't Group, Inc., et al. v. Does 1-6*, No. 04-1241 (E.D. Pa. Oct. 13, 2004), RJN Ex. C, and *In Re: Copyright Infringement Cases With Doe Defendants Related to Civil Action Number 04-1239*, Case No. 04-CV-650-CN, Dkt. 17 (E.D. Pa. January 21, 2005), RJN Ex. D. Notably, it also appears that in similar case, some ISPs have agreed upon procedures with Plaintiff to allow for such notice. See *Achte/Neunte*, No. 1:10-cv-00453-RMC, Further Stipulation Between Plaintiff And Third-Party Comcast Cable Communications Management, LLC Governing Responses To Rule 45 Subpoena and The Court's March 23, 2010 Order (Dkt. No. 18).

CONCLUSION

Plaintiff has the right to seek legal redress for alleged copyright infringement, but it must follow the basic procedures and due process requirements applicable to all civil litigation. Failure to abide by these procedures is not only contrary to law, it puts the Doe defendants at a disadvantage where they will first lose their constitutionally protected anonymity, and then find settlement economically more feasible than litigation in a foreign jurisdiction, even though they may have committed no unlawful act or may otherwise have meritorious defenses.

Amici therefore respectfully urge this Court to grant TWC's motion to quash the subpoena issued to TWC, and to quash, *sua sponte*, the similar subpoenas issued to other ISPs in this case. Additionally, we suggest that the Court instruct Plaintiff that any future subpoenas issued in this case to ISPs seeking the identity of anonymous Internet users must be accompanied by a cover notice ordering the ISP (1) to notify, within seven days of service of the subpoena, any person whose information has been sought that such information may be disclosed, and briefly describe their rights and options for protecting such information; and (2) to provide

sufficient opportunity for the subscriber to exercise those rights, such as by moving to quash. Plaintiff may be required to compensate the ISP for additional costs, if any, associated with providing notice.

Amici further respectfully suggest that the Court cure Plaintiff's improper joinder of the thousands of defendants named in this case by severing all but Defendant Doe 1 and "drop[ping]" Does 2 through 2000 from this action. Plaintiff may, of course, file new lawsuits in this District against any defendant, including Does 2-2000, as to whom Plaintiff can meet its burden of establishing jurisdiction.

Dated: June 2, 2010

Respectfully submitted,

s/Corynne McSherry

Corynne McSherry (CA 221504)

corynne@eff.org

Jennifer Granick

jennifer@eff.org

ELECTRONIC FRONTIER FOUNDATION

454 Shotwell Street

San Francisco, CA 94110

T: (415) 436-9333

F: (415) 436-9993

www.eff.org

Attorney for *Amicus*

ELECTRONIC FRONTIER FOUNDATION

s/Marcia Hofmann

Marcia Hofmann (D.C. Bar No. 484136)

marcia@eff.org

ELECTRONIC FRONTIER FOUNDATION

454 Shotwell Street

San Francisco, CA 94110

T: (415) 436-9333

F: (415) 436-9993

www.eff.org

Attorney for *Amicus*

ELECTRONIC FRONTIER FOUNDATION

Paul Alan Levy

pleavy@citizen.org

PUBLIC CITIZEN LITIGATION GROUP

1600 - 20th Street, N.W.

Washington, D.C. 20009

T: (202) 588-1000

<http://www.citizen.org/litigation>

Attorney for *Amicus*:

PUBLIC CITIZEN

Arthur B. Spitzer (D.C. Bar. No. 235960)
artspitzer@aol.com
AMERICAN CIVIL LIBERTIES UNION OF
THE NATION'S CAPITAL
1400 20th Street, N.W., Suite 119
Washington, D.C. 20036
T. 202-457-0800
F. 202-452-1868
www.aclu-nca.org

Attorney for *Amicus*:
AMERICAN CIVIL LIBERTIES UNION OF
THE NATION'S CAPITAL

Aden J. Fine (D.C. Bar No. 485703)
afine@aclu.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
T: (212) 549-2500
F: (212) 549-2651
www.aclu.org

Attorney for *Amicus*:
AMERICAN CIVIL LIBERTIES UNION