

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

USDC SDNY
DOCUMENT
ELECTRONICALLY FILED
DOC #:
DATE FILED: 3/28/12

PRO SE OFFICE

DIGITAL SIN, INC. :
 :
Plaintiff, :
 :
v. :
 :
JOHN DOES 1-176, :
 :
Defendants. :

Civil Action No.: 12-cv-00126-AJN

**MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT JOHN DOE'S
MOTION TO SEVER DEFENDANTS FOR IMPROPER JOINDER
AND TO VACATE THE ORDER GRANTING LEAVE TO SERVE
THIRD-PARTY SUBPOENAS AND TO QUASH THE SUBPOENA
AND FOR A PROTECTIVE ORDER**

FILED
U.S. DISTRICT COURT
12 MAR 29 P 4:03
S.D. OF N.Y.

Pursuant to Federal Rules of Civil Procedure (FED. R. CIV. P.) 20 and 21, Defendant, John Doe (“Defendant”), respectfully submits this Memorandum of Law in support of Defendant’s Motion to Sever Defendants for Improper Joinder and to Vacate the Order Granting Leave to Serve Third-Party Subpoenas and to Quash the Subpoena and for a Protective Order (“Motion”). In its motion, Defendant seeks 1) severance of the defendants for improper joinder and 2) that the Order dated January 30, 2012 granting Plaintiff, Digital Sin, Inc. (“Plaintiff”) leave to serve third-party subpoena upon the Internet Service Providers (“ISPs”), Sprint PCS, Verizon Internet Services, Road Runner, EarthLink, Clearwire Corporation, and Charter Communications be vacated and 3) that the subpoena be quashed, and 4) for a Protective Order.

I. INTRODUCTION

The instant case is part of a systemic effort to build a business model based on weak allegations of copyright infringement and questionable use of the legal system to quickly wrest profit through the generation of settlements from defendants cowed by the potential threat of a massive award of statutory damages (if Plaintiff’s joint and several theories are to be credibly believed, could allegedly result in excess of several millions of dollars based solely on weak allegations of what can only be described at best, as *de minimus* acts), attorneys fees, ignorance about defenses, and perhaps most importantly, the stigma which attaches to defendants when identified and associated with illegally downloading pornographic films to coerce quick, and profitable contingency-fee settlements. *See* Michael Roberts, *BitTorrent Motion Alleges Legal Business Model Targeting Porn Downloaders*, Denver Westword, September 16, 2011, http://blogs.westword.com/latestword/2011/09/porn_downloaders_bittorrent_lawsuit.php, attached hereto as Exhibit A.

As the Honorable Roger Hunt, Chief Judge of the U.S. District Court for the District of Nevada noted, similar plaintiffs “have attempted to create a cottage industry of filing copyright claims, making large claims for damages and then settling claims for pennies on the dollar, with defendants who do not want to incur the costs of defending the lawsuits.” *Righthaven LLC v. Democratic Underground, LLC*, No.2:10-cv-01356, Dkt. 94 (D. Nev. Apr. 14, 2011).

In perhaps the most explicit demonstration and subsequent repudiation of plaintiffs for profit litigation model, Magistrate Judge Beeler of the U.S. District Court for the Northern District of California, directly rebuked the plaintiff, in a similar case involving 188 John Doe defendants stating:

[t]he court has no confidence that Plaintiff has been diligent in moving to name and serve defendants, despite its (unsworn) claims to the contrary. For example, Plaintiffs counsel states that he has filed ten other copyright cases involving a large number of Doe defendants. ECF No. 17 at 4. The court reviewed the dockets and noted that the plaintiffs in these cases have not filed proof of service for even a single defendant even though a number of defendants have been identified and dismissed after settling with the plaintiffs. *See, e.g., Media Products, Inc. DBA Devil's Film v. Does 1-1257*, Case No. CV 10-04471 RS (complaint filed on October 4, 2010 and no proof of service filed for any defendant as of July 29, 2011, but four Doe defendants have been dismissed after settling). This pattern holds true in this case too. Here, Plaintiff has not identified or served any of the 1,219 Doe Defendants. However, on May 10, 2011, Plaintiff filed a stipulation dismissing with prejudice a Doe Defendant who settled with Plaintiff. ECF No. 13 at 1. And, on August 18, 2011, Plaintiff filed a stipulation dismissing with prejudice more than thirty Doe Defendants who settled. ECF No. at 1-2. The plaintiffs in these cases appear content to force settlements without incurring any of the burdens involved in proving their cases. And, while the courts favor settlements, “filing one mass action in order to identify hundreds of doe defendants through pre-service discovery and facilitate mass settlement, is not what the joinder rules were established for.” *IO Group, Inc. v. Does 1-435*, No. C 10-4382 SI, 2011 WL 445043, at *6 (N.D. Cal. Feb. 3, 2011).

Order Dismissing Complaint, *Patrick Collins Inc, V. Does 1-1,219*, Case 4:10-cv-04468-LB, Dkt. 27, at 4 (N.D. Cal. Aug. 29, 2011). Courts have specifically and directly condemned such for-profit copyright litigation models. See e.g., *Righthaven LLC v. Hill*, No. 1:11-CV-00211, Dkt. 16 (D.Colo. Apr. 7, 2011) (“Plaintiff’s wishes to the contrary, the courts are not merely tools for encouraging and exacting settlements from Defendants cowed by the potential costs of litigation and liability”).

In a similar civil action, prior to quashing all subpoenas and issuing an order to show cause to why the plaintiff’s and its counsel should not be sanctioned, a federal court described the underlying conduct as follows:

This course of conduct indicates that the plaintiffs have used the offices of the Court as an inexpensive means to gain the Doe defendants’ personal information and coerce payment from them. The plaintiffs seemingly have no interest in actually litigating the cases, but rather simply have used the Court and its subpoena powers to obtain sufficient information to shake down the John Does. Whenever the suggestion of a ruling on the merits of the claims appears on the horizon, the plaintiffs drop the John Doe threatening to litigate the matter in order to avoid the actual cost of litigation and an actual decision on the merits.¹

Likewise, in describing the behavior of the plaintiff prior to dismissing its action in a similar case, the Honorable Judge Beeler of the U.S. District Court for the Northern District of California, elucidated that the “plaintiffs in these cases appear content to force settlements without incurring any of the burdens involved in proving their cases,” and that the Plaintiffs have been abusing the court system in order to facilitate their scheme.² The Eastern District of Virginia issued an almost identical ruling regarding Raw Films, Ltd., and required Raw Films

¹ Memorandum Order, *K-Beech, Inc., v John Does 1-85*, No. 3:11cv469-JAG (E.D. Va., Oct. 5, 2011).

² Order Dismiss. Comp., *Patrick Collins, Inc, v. Does 1-1,219*, Case 4:10-cv-04468-LB (D. Cal. Aug. 29, 2011).

and its counsel to show cause as to why it should not be sanctioned.³ Indeed, there is no shortage of cases across the country where similar plaintiffs, have had their complaints dismissed or severed, had the subpoenas quashed, and face sanctions for engaging in frivolous litigation.⁴

Plaintiff in this case is no exception. It has filed similar mass-copyright infringement lawsuits against doe defendants, seeking settlements from innocent defendants. As of March 2012, Digital Sin, Inc. had filed 9 similar lawsuits against more than 7,000 individual John Doe Defendants.⁵ The Plaintiff's joining of 176 defendants in this action is an abuse of the judicial system. The only unifying factor in this case and only alleged reason for joining the defendants is defendants allegedly all utilized BitTorrent. BitTorrent is a file sharing protocol, which Plaintiff alleges the Doe defendants used to share and commit copyright infringement on a pornographic film. As the Northern District of California⁶ and District of Arizona⁷ held in dismissing similar actions, the notion of utilizing the same peer-to-peer network such as through BitTorrent is insufficient to justify the joining of numerous defendants in a single suit. In this present action, the Plaintiff alleges that the separate defendants shared a pornographic film in separate and isolated incidents that spanned the course of over 45 days.

The real reason for joining 176 defendants in a single suit, however, is not because the defendants allegedly engaged in tortious conduct together--rather, it is so the Plaintiff can

³ *Raw Films, Ltd., v John Does 1-32*, No. 3:11cv532 (E.D. Va., Oct. 5, 2011). It is also worth noting that federal courts have sanctioned Patrick Collin's counsel upwards of \$10,000.00 for filing unauthorized and improper subpoenas. See, e.g., *Mick Haig Productions, e.K., v Does 1-670*, No. 3:10-CV-1900-N (N.D.Tex. Sept. 9, 2011).

⁴ *Id.*; Order Dismiss. Comp., *Digiprotect USA Corp. v. Does 1-266*, No. 10 Civ. 8759 (S.D.N.Y., 2011); Order, *Patrick Collins, Inc. v Does 1-118*, No. 3:10-CV-92 (N.D.W.V. 2010); *Patrick Collins, Inc. v Does 1-281*, No. 3:10-CV-91 (N.D.W.V. 2010)(all defendants except Doe 1 severed and all subpoenas quashed); *Digiprotect USA Corp. v. Does 1-240*, No. 10 Civ. 8760 (S.D.N.Y., 2011) (dismissing action and closing case); *Diabolic Video Productions, Inc. v Does 1-2099*, No. 10-cv-5865-PSG (N.D. Cal, 2010) (severing all defendants against Doe 1); *Raw Films, Ltd., v John Does 1-32*, No. 3:11cv532 (E.D. Va., Oct. 5, 2011)(severing all defendants and quashing all subpoenas, and ordering plaintiff to show cause as to why it should not be sanctioned).

⁵ This data is based on a PACER search of all federal courts for Digital Sin as a party.

⁶ Order, *Hard Drive Productions, Inc., v Does 1-188*, No. C-11-01566 JCS (severing all defendants and quashing all subpoenas)

⁷ Order, *Patrick Collins, Inc., v John Does 1-54*, No. CV-11-1602-PHX-GMS (severing defendants)

circumvent having to file separate lawsuits in the proper venue and avoid having to pay separate filing fees. Indeed, for the Plaintiff, it is the difference in paying \$350.00 as a filing fee for this action, or paying \$61,600.00 in filing fees had the case been filed properly against the 176 defendants separately. Likewise, the Plaintiff's strategy relies on making fighting an action as costly as possible for the defendants. By taking a shotgun approach and attacking a vast number of defendants, Plaintiff can ensure economic feasibility of its deplorable lawsuits so long as a few defendants settle the matter.

In light of the obvious abuse of the judicial system as well as the significant risk of misidentification of potential defendants as discussed below, Doe Defendants 2-176 should be severed from this action and the Order granting leave to serve third-party subpoenas should be vacated and the subpoena should be quashed.

II. ARGUMENT

A. Joinder of Defendants Is Improper

Plaintiff has not and cannot bind together the 176 individuals who make up the John Does in this case. It is difficult to envision a situation where bringing suit against 176 separate defendants in a single suit would be proper. While the courts generally allow the joining of parties for claims involving the same transaction and occurrence in the interest of facilitating judicial economy, judicial economy is not facilitated by joinder in this action: only the Plaintiff's economic interest is facilitated by joining 176 defendants in this suit. Aside from the fact that Plaintiff falsely alleges that Defendant traded a part of a pornographic movie using BitTorrent, the defendants do not share any common facts or interests. Defendant respectfully requests that this Court sever all but John Doe 1 from the action for improper joinder of

defendants.

1. Legal Standard

Pursuant to FED. R. CIV. P. 20(a)(2), permissive joinder of defendants is proper 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(a)(2). *See also Cooper v. Fitzgerald*, 266 F.R.D. 86, 88 (E.D. Pa. 2010) (Kelly, J.). Permissive joinder is “designed to promote judicial economy and trial convenience.” *Hard Drive Productions, Inc. v. Does 1-188*, 809 F. Supp. 2d 1150, 1156 (N.D. Cal. 2011). *See also Mosley v. General Motors Corp.*, 497 F.2d 1330, 1332-33 (C.A. Mo. 1974) (*citing* 7 C. Wright, *Federal Practice and Procedure* § 1652 at 265 (1972)). Even if FED. R. CIV. P. 20(a)’s requirements are met, “a district court must examine whether permissive joinder would ‘comport with the principles of fundamental fairness’ or would result in prejudice to either side.” *Hard Drive Prods.*, 809 F. Supp. 2d at 1156. Rule 21 further provides that upon finding misjoinder of parties, upon motion or on its own, a court may, at any time, add or drop a party. *See* FED. R. CIV. P. 21.

2. Plaintiff Has Failed to Meet the Requirements of Rule 20(a) and Doe Defendants 2-176 Should Be Severed From This Action

Joinder is improper because Plaintiff has failed to establish that the claims arise out of the same transaction, occurrence or series of transactions or occurrences, and contain common questions of law or fact. The claim that joinder is proper based on Internet file sharing protocols like BitTorrent or other peer-2-peer (“P2P”) protocols has been reviewed and almost universally

rejected by various courts. *See Fonovisa, Inc. v. Does 1-9*, 2008 WL 919701 (W.D. Pa. April 3, 2008) (finding joinder improper because of the different factual contexts of the alleged infringement for each defendant and absence of any evidence showing joint action by defendants, other than their use of the same Internet file sharing network to access copyrighted recordings); *LaFace Records, LLC v. Does 1-38*, 2008 WL 544992 (E.D.N.C. Feb. 27, 2008) (rejecting joinder based on the claim that defendants used the same ISP and P2P network to allegedly commit copyright infringement); *Diabolic Video Productions, Inc. v. Does 1-2099*, 2011 WL 3100404 (N.D. Cal. May 31, 2011) (holding that the nature of the Internet file sharing protocol, BitTorrent, does not make joinder appropriate where defendants allegedly used Internet file sharing to infringe copyrighted works); *K-Beech, Inc. v. John Does 1-85*, 2011 WL 4915551 (E.D. Va. Oct. 17, 2011) (“mere allegations that Doe Defendants have used the same peer-to-peer network to copy and reproduce their videos is insufficient to meet the standards of joinder.”); and *Patrick Collins, Inc. v. Does 1-118*, Case 3:10-CV-92-JPB, Dkt. 42 (N.D.W.Va. Dec. 16, 2010).

Despite Plaintiff’s claims, based on and according to the great weight of judicial authority, the Doe Defendants did not participate in the same transaction or occurrence, or the same series of transactions or occurrences, as required for joinder; nor, did they act in concert with one another. The mere fact that any of the Doe Defendants may have allegedly clicked on a command to participate in the internet file sharing network does not mean that each, together, was part of the downloading done by hundreds or thousands of individuals.

Just last week, in a similar mass copy-right infringement action, District of Arizona Judge G. Murray Snow severed the 2 remaining defendants, John Doe 6 from John Doe 12, finding that the joinder was improper. Judge Snow noted in his order that:

Plaintiff alleges that the two remaining Defendants “participat[ed] in the BitTorrent swarm with other infringers” but does not claim that John Doe 6 provided data to the former John Doe 12 or vice versa. (Doc. 26 ¶ 56). Plaintiff included as Defendants only those IP addresses from the swarm in question that were located in Arizona, demonstrating that the actions of the individual members of the swarm are easily distinguishable. Plaintiff alleges no facts that these two particular Defendants shared data with each other, and provides data instead that they were logged on to BitTorrent weeks apart.⁸

In the instant action, Plaintiff similarly alleges no facts that any of the 176 Defendants shared data with each other or any facts that would lead one to believe that the defendants acted in concert, worked together, or took any action that would constitute the same transaction or occurrence, instead provides data that the Defendants were logged on to BitTorrent more than 6 weeks apart. The only similarity is that defendants allegedly infringed on the same pornographic movie, albeit on different days and different times.

In the instant action, Plaintiff’s crucial allegation that defendants are “likely within the same “swarm”” is unsupported and Plaintiff proffers a sample of what a swarm is suppose to be like, instead of offering evidence of the alleged actual swam in this case. Instead the Plaintiff suggested tenuously that by specifically limiting the time period during which the investigated alleged downloads occurred ensured commonality amongst the alleged infringers. Thus the alleged infringers were likely within the same swarm and engaged in a series of related transactions. This fallacy is central to the Plaintiff’s case for joinder. This is akin to saying that because 176 thieves who shoplifted the same brand of chocolate bars in the same supermarket over a specifically limited 6 week period they must be acting in concert and related.

Examining the DigiProtect cases in Southern District of New York, also explicitly rejected the reasons asserted for joinder in this instant action. As discussed by Judge Crotty:

⁸ Order, *Patrick Colins, Inc., v John Does* 1-54, No. CV-11-1602-PHX

For the same reasons, DigiProtect cannot join hundreds of individuals in a single case by alleging that they infringed the same copyright by illegally downloading the same movie, albeit in separate instances. The swarming capacity of peer-to-peer networks alone does not mean that John/Jane Does actually engaged in "the same transaction, occurrence, or series of transactions or occurrences," as required by Fed. R. Civ. P. 20(a)(2)(A). ... Any repleading by DigiProtect must be based on specific factual allegations connecting these defendants to the same specific swarming transaction, or series of transactions, to support their joinder. Otherwise, the only "commonality" is that "each commit[ted] the exact same violation of the law in exactly the same way." The current allegations are inadequate to support joinder.

Digiprotect USA Corp. v. Does 1-240, No. 10 Civ. 8760, fn 3 (S.D.N.Y., 2011)(internal quotations and citations omitted). As highlighted above, the Plaintiff did not make specific factual allegations connecting the Defendants to the same specific swarming transaction, nor offer any evidence that the Defendants were of the same swarm and shared parts of the alleged copyrighted work with each other.

Nonetheless, allegations that the defendants are part of the same "swarm" for any alleged file sharing, which would confer joinder, has been expressly rejected by Courts throughout the country as a basis of conferring joinder.⁹

Moreover, even if it were true that all Doe Defendants participated in what Plaintiff describes as a "swarm," it cannot be said that each defendant was physically present at the same day and time. In fact, Plaintiff admits that downloading was done at different times and dates ranging throughout a 6-week period from October 29, 2011 to December 13, 2011.

Also as stated above, in another similar mass-copyright infringement action, Judge Timothy J. Savage severed all but one defendant from the action, finding that the joinder of the various defendants was improper. Judge Savage noted that "even assuming as true plaintiff's allegation that the Does downloaded and shared the same file and were part of the same swarm, permissive joinder is in appropriate given the nearly two-month period during which the Does

⁹ See e.g., *K-Beech, Inc., v John Does 1-85*, No. 3:11 cv469-JAG (E.D. Va., Oct. 5, 2011).

allegedly downloaded the Work.” *Id.* at n. 1 (citing *Hard Drive Prods. v. Does 1-33*, No. C. 11-03827 LB, 2011 WL 5325530, at *3 (N.D. Cal. Nov. 3, 2011) (holding joinder of thirty-three swarm members inappropriate given a similarly disparate range of alleged infringement dates)).

Given the fact that Plaintiff in this action similarly alleges that 176 Does downloaded and shared the same file and were part of the same swarm over a 6-week period, permissive joinder should likewise be deemed inappropriate in this matter and all Doe Defendants 2-176 should be severed from this action.

3. Joinder Is Not Appropriate and Doe Defendants 2-176 Should Be Severed From This Action

Even if, *arguendo*, Plaintiff has met the requirements set forth under FED. R. CIV. P. 20(a), the joinder is nevertheless not appropriate and Doe Defendants 2-176 should be severed from this action because the joinder of the Doe Defendants would defeat judicial economy, result in a series of mini-trials, go against notions of fundamental fairness, and ultimately cause prejudice to defendants.

In *Hard Drive Prods.*, *supra*, the court found that permitting joinder was not only impracticable, but would “undermine Rule 20(a)’s purpose of promoting judicial economy and trial convenience because it would result in a logistically unmanageable case.” *Hard Drive Prods.*, *supra*, 809 F.Supp.2d at 1164 (citing *Bridgeport Music, Inc. v. IIC Music*, 202 F.R.D. 229, 232-33 (M.D. Tenn. 2001)). The court also found that:

... permissive joinder of the Doe Defendants does not comport with the “notions of fundamental fairness,” and that it will likely cause prejudice to the putative defendants. *See Coleman*, 232 F.3d at 1296. The joinder would result in numerous hurdles that would prejudice the defendants. For example, even though they may be separated by many miles and have nothing in common other than the use of BitTorrent, each defendant must serve each other with

all pleadings—a significant burden when, as here, many of the defendants will be appearing *pro se* and may not be e-filers. Each defendant would have the right to be at each other defendant's deposition—creating a thoroughly unmanageable situation. The courtroom proceedings would be unworkable—with each of the 188 Does having the opportunity to be present and address the court at each case management conference or other event. Finally, each defendant's defense would, in effect, require a mini-trial. These burdens completely defeat any supposed benefit from the joinder of all Does in this case, and would substantially prejudice defendants and the administration of justice.

Hard Drive Prods., 809 F. Supp. 2d at 1164.

Likewise, in the other mass-copyright infringement case currently pending before Judge Timothy J. Savage, the Court (*citing Hard Drive Prods. v. Does 1-188*) determined that even if plaintiff had met the requirements of Rule 20(a), “it is appropriate to sever and dismiss all but one Doe.” *See* Order (Savage, J.). In granting severance, the Court found that in spite of the similar conduct allegedly perpetrated by the defendants, different defenses have been presented and are likely to be presented should joinder remain. *Id.* (Savage, J.) (*citing BMG Music v. Does 1-203*, 2004 WL 953888, at *1 (E.D. Pa. Apr. 2, 2004) (Newcomer, J.) (describing a similar scenario where “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 Doe 3 through 203 could be thieves, just as Plaintiffs believe.”)).

Because the Plaintiff has not even made a *prima facie* showing that joinder is proper, as the Supreme Court has indicated, discovery pertaining to the defendants must not be allowed to proceed in this action. Indeed, the underlying rationale elucidated by the Supreme Court is applicable here: namely, allowing this matter to proceed will allow a largely groundless claim to take up the time of a number of people, and shall represent an *in terrorem* increment of this

action's settlement value.¹⁰

Additionally, at a minimum, when a party is misjoined in an action, any claim against a party should be severed and proceeded with separately.¹¹ As one example, in a West Virginia action, the District Court severed the action against all Doe defendants.¹² The West Virginia Court elucidated that evidence of misjoinder is found in the undeniable fact that, among others, each defendant would have completely separate and distinct factual scenarios surrounding each alleged infringement.¹³ The West Virginia Court subsequently severed all defendants in the lawsuit, quashed all subpoenas except the subpoena for John Doe 1, and allowed the Plaintiff to file amended complaints (and required separate filing fees) regarding the remaining 117 Doe defendants.¹⁴

Similarly, in light of the different defenses that are likely to be presented and the substantial prejudice to defendants, the Court should likewise sever the action as to Doe Defendants 2-176.

**B. Order Granting Permission to Serve Subpoena Should Be Vacated
and the Subpoena Should Be Quashed**

A Rule 45 subpoena must fall within the scope of proper discovery under Federal Rule of Civil Procedure 26(b)(1), which limits discovery to “any matter, not privileged, that is relevant to the claim or defense of any party in the pending action and is reasonably calculated to lead to the discovery of admissible evidence.” Fed. R. Civ. P. 26(b)(1). If a subpoena falls outside the scope

¹⁰ *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 558 (2007); *Ashcroft v. Iqbal*, 129 S.Ct. 1937, 1950 & 1953 (2009).

¹¹ See Fed. R. Civ. P. 21.

¹² Order, *Patrick Collins, Inc. v Does 1-118*, No. 3:10-CV-92 (N.D.W.V. 2010).

¹³ *Id.*

¹⁴ Order, *Patrick Collins, Inc. v Does 1-118*, No. 3:10-CV-92 (N.D.W.V. 2010); see *BMG Music v. Does 1-203*, 2004 WL 953888 (E.D. Pa. Apr. 2, 2004).

of permissible discovery, the Court has authority to quash or modify it upon a timely motion by the party served, or a party challenging the relevancy of, or claiming a privacy interest in, the records sought. *See* Fed. R. Civ. P. 45(c) (3).

This Court, in its Order Granting Plaintiff's Motion for Leave to take Discovery Prior to Rule 26(f) Conference, explicitly recognized Defendants' right to challenge the Subpoena. The Subpoena issued to the ISPs should be quashed pursuant to Rule 26 of the Federal Rules of Civil Procedure because Defendant: (1) challenges the legal sufficiency and legitimacy regarding Plaintiff's request for early discovery that produced the Subpoena, for which Defendant was never given notice or an opportunity to be heard, and (2) claims a privacy interest in the records sought.

**1. Defendant Has Standing to Challenge the Subpoena Because
Defendant Has a Personal Interest in the Subpoenaed Matter**

A party has standing to challenge a subpoena issued to a third party when the party has a personal right or privilege in the information sought by the subpoena. *See Kida v. EcoWater Systems LLC*, 2011 WL 1883194, *2 (E.D. Pa. 2011) (Baylson, J.). Here, because the subpoena issued to the ISPs seek Defendant's personal identifying information, Defendant undoubtedly has a "personal right" in the information sought by the subpoena. Further, once Defendant's name is turned over by the ISPs, Plaintiff, as part of its business-model will quickly seek settlements from any identified Doe Defendants, amounting to thousands of dollars each, with no serious intention of naming any Defendant and litigating the matter on the merits. If an identified Doe Defendant has a personal right sufficient to pay several thousands of dollars under the threat of public exposure and litigation, certainly Defendant has a personal right sufficient to object prior to that disclosure. Accordingly, Defendant has standing to challenge the subpoena.

2. The Order Granting Leave to Serve Third-Party Subpoena Should Be Vacated

In addition to the fact that the defendants have been improperly joined, the Order granting leave to serve third-party subpoenas should be vacated because the technology utilized to identify individual defendants for the alleged copyright infringement is unreliable and insufficient to show a volitional act of copyright infringement.¹⁵ More specifically, there is not only software capable of impersonating and/or falsifying an IP address (“spoofing”)¹⁶, but such tracing software is unreliable because the software is incapable of detecting MAC addresses. Furthermore, most ISPs do not store MAC address data and they have no ability to detect MAC addresses that have been falsified. Because the technology utilized by Plaintiff to “identify” Defendant is undoubtedly unreliable, Plaintiff is surely incapable of accurately verifying individuals who downloaded copyrighted material, and from where the material is downloaded. Because IP addresses indicated on Plaintiff’s subpoenas are unreliable, Plaintiff cannot base its subpoenas on such unreliable information.¹⁷ Moreover, to prove infringement, a plaintiff must first prove that the defendant copied the protected work (*see Kelly v. Arriba Soft Corp.*, 336 F.3d 811, 817 (9th Cir. 2003) (“the plaintiff must show ownership of the copyright and copying by the defendant”)), and that the copying was a result of a volitional act. *See Religious Tech. Ctr v. Netcom On-Line Commc’n Servs., Inc.*, 907 F. Supp. 1361, 1369-70 (N.D. Cal. 1995). However, Plaintiff’s allegations are woefully inadequate and do not, and cannot account for numerous issues, from open wireless networks being illegally invaded, IP address spoofing to human and

¹⁵ See James Temple, *Stelle Hansmeier drops suit against ‘porn granny’*, San Francisco Chronicle, Aug. 31, 2011, <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/08/31/BUAC1KTB44.DTL>, attached hereto as Exhibit B.

¹⁶ See e.g., <http://Proxy.org/>.

¹⁷ A more thorough discussion of BitTorrent technology can be found in *Boy Racer, Inc. v. Doe*, 2011 WL 3652521 (N.D. Cal. 2011).

collection errors. Courts again have touched on this simple yet utterly logical idea: *an IP address is not a Copyright Infringer*. As the Central District of Illinois Court noted:

[Plaintiff] ignores the fact that IP subscribers are not necessarily copyright infringers. Carolyn Thompson writes in an MSNBC article of a raid by federal agents on a home that was linked to downloaded child pornography. The identity and location of the subscriber were provided by the ISP. The desktop computer, iPhones, and iPads of the homeowner and his wife were seized in the raid. Federal agents returned the equipment after determining that no one at the home had downloaded the illegal material. Agents eventually traced the downloads to a neighbor who had used multiple IP subscribers' Wi-Fi connections (including a secure connection from the State University of New York).

VPR Internationale v. Does 1-1017, Case No. 2:11-cv-02068-HAB, Dkt. 15, at 2 (C.D. Ill April 29, 2011). However, "whether you're guilty or not, 'you look like a suspect.'" *Id.* at 3.

Plaintiff has misled this Court by suggesting that it will be able to identify the Defendants through issuance of subpoenas to the ISPs. This suggestion is inaccurate.

An IP address can only identify a subscriber to an ISP; it does not identify the specific identity of the person that actually engaged in the alleged infringing activities. To successfully identify the claimed infringers, Plaintiff would need extensive additional information that cannot be gleaned from information requested by the Subpoena. Indeed, Plaintiff's inaccurate portrayal of the facts required to identify infringers was exposed in a similar lawsuit just three months ago, *Boy Racer, Inc. v. Does 1-52*, No. 11-CV-2329-PSG (N.D. Cal. Sept. 13, 2011) (order denying further discovery; order to show cause).

In that case, after issuing a substantially identical subpoena and representing to the court that each IP address corresponded to a defendant, the plaintiff was forced to admit that the subscriber information linked to an IP number was legally insufficient to identify a defendant and really just the starting point for a far more invasive investigation. In rejecting that

plaintiff's attempt to expand its discovery beyond its initial representations, the court quoted the key admissions to the plaintiff's argument as follows:

While Plaintiff has the identifying information of the subscriber, this does not tell Plaintiff who illegally downloaded Plaintiff's works, or, therefore, who Plaintiff will name as the Defendant in this case. It could be the Subscriber, or another member of his household, or any number of other individual who had direct access to Subscribers network.

[Accordingly:]

Plaintiff plans to request a limited inspection of Subscriber's electronically stored information and tangible things, such as Subscriber's computer and the computers of those sharing his Internet network, for the purpose of finding the individual that unlawfully violated Plaintiff's copyrighted works by uploading/downloading the file referenced BitTorrent, or to see whether such information has since been erased contrary to instructions by Verizon Online and Plaintiff's attorneys.

Id. at 4 (withdrawing its prior order granting limited early discovery and denying further discovery requests because “[p]resumably, every desktop, laptop, smartphone, and tablet in the subscriber's residence, and perhaps any residence of any neighbor, houseguest or other sharing his internet access, would be fair game”) (internal quotes and citations omitted).

The only factual support that Plaintiff provides for the allegations in the Complaint are a list of IP addresses from which it is alleged infringing activity took place, supplied by Copyright Enforcement Group, LLC (“CEG”) and the Declaration of John Nicolini, CEG's Vice President, attesting to the highly technical computer-based applications and methodology which he claims identify the Defendants as alleged infringers. However, this Court must heavily discount, if not dismiss, any evidentiary support these items may lend to Plaintiff's Complaint upon information and belief CEG is actually an interested party in this litigation, rather than an independent witness as Plaintiff would have this court believe.

It is widely accepted that “it is improper for an expert to be compensated on a contingent fee basis.” Michael H. Graham, 5 Handbook of Fed. Evid. § 702:3 (7th ed.); see *Person v. Ass’n of the Bar of the City of New York*, 554 F.2d 534 (2d Cir. 1977); *Swafford v. Harris*, 967 S.W. 2d 319 (Tenn. 1988); *Dupree v. Malpractice Research, Inc.*, 445 N.W. 2d 498 (Mich. 1989); *Polo v. Gotchel*, 542 A.2d 947 (N.J. 1987). “An agreement to give an opinion on a contingent basis, particularly on an arithmetical scale, attacks the very core of expert testimony.” *Gediman v. Sears, Roebuck & Co.*, 484 F.Supp. 1244, 1248 (D. Mass. 1980). Such an agreement is classified by Williston on Contracts, 3d ed. 1972, Section 1716 under “Bargains Obstructing Justice.” See also, Restatement of the Law, Contracts, 1932 § 552(2).

While acknowledging that Plaintiff is a client of CEG, neither Plaintiff nor Declarant Nicolini ever specifies to the court how CEG, and thus the Declarant, were compensated. A brief review of CEG's website reveals that their services are offered “at no cost to content owners.” Copyright Enforcement Group, Monetization, <http://www.ceg-intl.com/monetization.html> [Attached hereto as Exhibit C and incorporated by reference herein as if set forth verbatim herein]; also Press Release, Copyright Enforcement Group, New-Anti Piracy Solutions and Business Intelligence Services Launched by Copyright Enforcement Group (CEG) (Jan. 11, 2012), <http://www.prweb.com/pdfdownload/9087878.pdf> (“available at no cost to content owners”) [Attached hereto as Exhibit D and incorporated by reference herein as if set forth verbatim herein]. The only reasonable explanation for this “no cost” service is that CEG is being compensated from a percentage of the settlements and/or judgments resulting from this litigation.

The opacity of how Plaintiff and Declarant treat this issue is particularly alarming. As one court noted: “[t]he concealment of a contingent financial arrangement with a witness would be unconscionable. With the disclosure of such an arrangement, an opinion proffered by an

expert would likely be so undermined as to be deprived of any substantial value.” *Creative Dimensions in Mgmt., Inc. v. Thomas Group, Inc.*, No. CIV. A. 96-6318, 1999 WL 135155, at *2 (E.D. Pa. Mar. 11, 1999).

Declarant's undisclosed financial interest in this litigation is likely one of the reasons that the Declaration did not address the error rate of the software used to identify Defendants, and erroneously concluded that Defendants, as ISP subscribers, were the individuals involved in copyright infringement activity.

The Declaration would have this Court believe that CEG's highly technical methods used to identify IP addresses from which allegedly infringing activity took place are highly accurate, but recent studies have shown that similar software produces a large number of false positives. A recent study performed by the Department of Computer Science and Engineering at the University of Washington determined that “copyright holders utilize inconclusive methods for identifying infringing BitTorrent users. [The Researchers] were able to generate hundreds of DMCA takedown notices for machines under [their] control at the University of Washington that were not downloading or sharing any content.” Michael Piatek et al., *Challenges and Directions for Monitoring P2P File Sharing Networks –or– Why My Printer Received a DMCA Takedown Notice*, 3rd USENIX Workshop on Hot Topics in Security 2008, (July 29, 2008) http://www.usenix.org/event/hotsec08/tech/full_papers/piatek/piatek.pdf. Specifically, the article concludes:

[W]e find that it is possible for a malicious user (or buggy software) to implicate (frame) seemingly any network endpoint in the sharing of copyrighted materials. We have applied these techniques to frame networked printers, a wireless (non-NAT) access point, and an innocent desktop computer, all of which have since received DMCA takedown notices but none of which actually participated in any P2P networks.

Id.

Also, and as noted above, the Declaration makes no accounting for actions engaged in by third parties using Defendants' networks. As one court noted in a similar case:

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. . . . Wholesale litigation of these claims is inappropriate, at least with respect to a vast majority (if not all) Defendants.

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

The undisclosed nature of CEG's compensation and the likelihood that it is in some way contingent upon this litigation strongly violates public policy and renders the Declaration and other evidentiary support produced by CEG so necessarily flawed that they cannot not assist this Court in determining the facts of this case. Plaintiff is attempting to obtain Defendant's Constitutionally protected information without even being able to create a prima facie record to support its allegations that any of the Defendants, engaged in or contributed to copyright infringement.

Plaintiff's claims and alleged IP evidence also fail to provide any evidence of liability under a theory of contributory infringement. Specifically, Plaintiff must show "[o]ne who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another." *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 264 (9th Cir. 1996) (citing *Gershwin Publishing Corp. v. Columbia Artists Mgmt., Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971)). See generally *Newborn v. Yahoo!, Inc.*, 391 F.Supp.2d 181 (D.D.C. 2005). Since as a matter of law, an IP address is not a person under any direct infringement analysis, it is simply logical by extension that an unreliably harvested IP address fails to allege any knowledge of or contribution to any infringing activity.

Based on the technological ease with which wholly innocent Defendants can be so easily falsely identified—for example when the neighbor, unbeknownst to anyone, illegally executing a BitTorrent protocol through a putative Defendant’s wireless signal, or perhaps a person simply accessing through increasingly popular free public “Wi-Fi”—coupled with the devastating effect such a false accusation could have, Plaintiff’s allegations fail to provide sufficient accuracy, nor a volitional act associated to an account holder sufficient to support its claim. Thus, the Order granting leave to serve third party subpoenas should be vacated and the subpoena should be quashed.

**3. The Subpoena Should Be Quashed to Protect Defendant From
Unreasonable Annoyance, Embarrassment and Oppression**

The Order granting leave to serve third-party subpoenas should be vacated and the subpoena quashed to prevent Defendant from suffering unwanted annoyance, embarrassment, and oppression, or otherwise, suffering an undue burden. *See* FED. R. CIV. P. 45(c)(3)(A)(iv). Here, Plaintiff, as part of its for-profit business model, seeks Defendant’s confidential personal identifying information from Defendant’s ISP so that Plaintiff can annoy and embarrass Defendant, and coerce a quick and profitable settlement under the threat of publicly outing Defendant of illegally downloading pornography—despite evidence calling into question whether Defendant ever engaged in such acts.

Plaintiff’s subpoena is intended to cause an undue annoyance, embarrassment, and oppression that would result if Defendant’s personal identifying information were associated, without sufficient evidentiary support, of illegally downloading pornography. Such association would be highly embarrassing to Defendant, unjustifiably stigmatizing to Defendant, injurious of the Defendant’s character and reputation, and potentially jeopardizing to the Defendant’s

employment. Moreover, even after Defendant is able to demonstrate that Plaintiff's allegations in this suit are false, the embarrassment and reputational damage from Plaintiff's false public claim will still persist. However, by vacating its Order granting Plaintiff leave to serve third-party subpoena and by quashing the Plaintiff's subpoena, the Court can prevent Defendant from being unjustly harmed and embarrassed by premature allegations of downloading illegal pornography. Under these circumstances, the Order should be vacated and the subpoena should be quashed.

C. Alternatively, a Protective Order Should Be Entered Precluding Public Disclosure of Defendant's Confidential Information

Alternatively, Defendant respectfully requests that the Court enter a protective order prohibiting the public disclosure of any confidential information relating to Defendant that is obtained from Defendant's ISP through the subpoena.

Under Rule 26(c), this Court is authorized to issue such a protective order "to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense, including . . . specifying terms . . . for the disclosure [and] limiting the scope of disclosure . . . as to certain matters." FED. R. CIV. P. 26(c)(1)(B) & (D).

Here, if the Court does not vacate the Order and does not quash Plaintiff's otherwise improper subpoena, the Court, at a minimum, should enter a protective order prohibiting the public disclosure of any information relating to Defendant obtained via the subpoena. Among other things, the protective order should mandate that all court filings in this action that contain or reference information relating to Defendant obtained via the subpoena must either be redacted or filed under seal to prevent the public disclosure and ensure the continued confidentiality of that information.

Such a public accusation would be highly embarrassing to Defendant, unjustifiably stigmatize Defendant, injure Defendant's character and reputation, and potentially jeopardize Defendant's employment. Moreover, even after Defendant is able to demonstrate that Plaintiff's allegations in this suit are false, the embarrassment and reputational damage from Plaintiff's false public claim will still persist. By entering the requested protective order, however, the Court can prevent Defendant from being unjustly harmed and embarrassed by premature allegations of downloading illegal pornography without impairing Plaintiff's ability to obtain the requested information and otherwise litigate its case.

Prohibiting public disclosure of Defendant's confidential information is necessary to prevent Defendant from suffering undue annoyance, embarrassment, and oppression that would result if Plaintiff, without sufficient evidentiary support, publicly accuses Defendant of illegally downloading pornography. In addition, such protection will comport with this Court role as an impartial adjudicator of legal disputes and not "merely tools for encouraging and exacting settlements from Defendants cowed by the potential costs of litigation and liability." *Righthaven LLC v. Hill*, *supra*, No. 1:11-cv-00211, Dkt. 16.

As noted *infra*, "the embarrassment of public exposure might be too great, the legal system too daunting and expensive, for some to ask whether [Plaintiff] has competent evidence to prove its case." *VPR Internationale*, *supra*, Case No. 2:11-cv-02068-HAB, Dkt. 15, at 3. Is it then illogical or unthinkable to think that an anonymous Defendant—irrespective of actual guilt or innocence—faced with the professional/personal ruin, along with the uncertainty and cost of a federal lawsuit wouldn't simply decide to pay a few thousand dollars to make "it" all go away? Such Protection Order furthers this appropriate judicial role and would not prejudice Plaintiff's rights in any way.

Accordingly, if the Court does not sever John Doe Defendants 2 through 176 from this action, does not vacate its Order and does not quash the Subpoena, the Court should enter a protective order: (1) prohibiting the public disclosure of any information relating to Defendant obtained from Defendant's ISP through Plaintiff's Subpoena without Defendant's consent or the Court's prior authorization; and (2) requiring any party filing a pleading in this action that contains or references any information relating to Defendant produced in response to the Subpoena to file under seal.

III. CONCLUSION

Plaintiff's instant action is an abuse of the judicial system and nothing more than an attempt to take advantage of the 176 defendants listed in this action. On one hand, Plaintiff attempts to circumvent traditional safeguards of civil procedure by joining, with tenuous allegations, defendants that share no common facts, while Plaintiff simultaneously avoids contributing to the judicial system by circumventing costly filing fees.

On the other hand, Plaintiff has attempted to extract low settlements from thousands of defendants, throughout the nation, in such a way that it makes little economic sense for the defendants to resist settling with the Plaintiff even if they did nothing wrong. cursory analyses of the other cases similar to this one indicate that the Plaintiff has no intention of actually pursuing a lawsuit against the defendants. Rather, the Plaintiff wants to simply threaten unsophisticated defendants with expensive litigation and the stigma of having their names tarnished by being associated with obscene pornographic movies. This Court should not condone or permit such activity.

For the reasons set forth above, Defendant respectfully requests this Court GRANT the

Defendant's Motion and provide Defendant the following relief:

- (1) Dismiss the Defendants, or in the alternate, sever Defendants due to Plaintiff's improper joinder of 176 defendants;
- (2) Quash the subpoena at issue;
- (3) To the extent a subpoena is not quashed, grant a protective order sealing and preventing the disclosure of any information obtained through a subpoena;
- (4) Sanction Plaintiff; and,
- (5) Provide any further relief to Defendants that is just and proper.

Respectfully submitted this 26th day of March, 2012.

/s/ John Doe

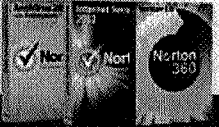
John Doe

Pro se

EXHIBIT A

Fast. Powerful. Effective. Norton 2012.
Get the #1-ranked online security that won't slow you down.

Shop Now



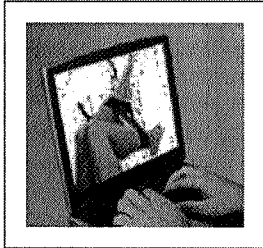
NEW

BitTorrent motion alleges legal business model targeting porn downloaders

By Michael Roberts

published: Fri., Sep. 16 2011 @ 12:13PM

Imagine receiving a letter from an attorney accusing you of illegally downloading a cinematic classic like, say, *The Godfather* or *The Man Who Blew Too Much*, but offering you a chance not to be accused of this offense in public court for a few thousand bucks. Would you take the deal? Plenty of people do. However, a BitTorrent motion filed in Colorado is taking on the practice, which one attorney refers to as "business-model litigation."



"The BitTorrent lawsuits are part of a systemic effort to build a business model based on weak allegations of copyright infringement and the inducement of fear," e-mails Christina Saunders, who filed the motion, accessible below, for one of 26 John Doe defendants targeted by Patrick Collins, Inc., a company owned by the prominent porn director of the same name. (His titles include *Cum Rain Cum Shine 2* and *Sodomania 32*.) "In my mind, they constitute as an abuse of copyright law, the judicial system, and they threaten the integrity and respect for the courts."



Patrick Collins.

In response, Jason Kotzker, attorney for Patrick Collins, Inc., says he can't speak at length about the case until after there's a ruling on Saunders's motion. But "in the interim, I can tell you that peer-to-peer copyright infringement in the aggregate is a major problem for my clients," he writes via e-mail, "and like any other copyright holder, they will protect their rights when infringement is discovered."

How does the approach work? David Kerr, a Saunders colleague and copyright-law expert who represented chronically ill hobby blogger Brian Hill after he was targeted by controversial Las Vegas firm Righthaven LLC for unauthorized use of a *Denver Post* photos, lays things out this way.

"After being hired by, say, a production company, a law firm, or a company it hires, will go into BitTorrent networks to find out who's downloading a certain movie, and then they'll harvest IP addresses," he notes. "They might come up with a list of twenty to 20,000 addresses -- and then they slap all of them into one lawsuit and file it with a court. They say, 'We think these people are infringers, but we don't know who they are. So we want you to allow us to send subpoenas to Internet service providers like Comcast to get the subscriber information that corresponds to that IP address."

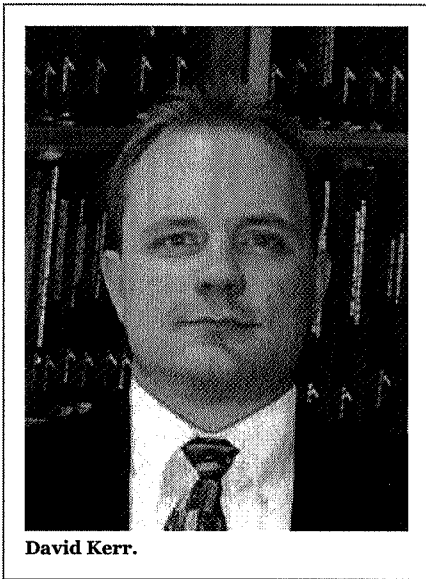
"Once the court gives the law firm permission, the attorney sends Comcast a subpoena... And after they turn over the names, the attorney sends a letter to these John Doe defendants that usually consists of something like, 'Pay us money, or we're going to sue you.' And the settlements usually range from \$3,500 to \$5,000 a pop."

Just because an individual's IP address came up in such a search doesn't mean he or she has actually downloaded the flick in question, Kerr stresses. "I've probably gotten 200 calls on these types of cases, and a lot of them involve open wireless. If my neighbor jumps on the wireless and downloads a movie,

it's going to show up on my IP address. That's happened to clubhouses, coffeehouses, neighborhood associations. And also, IP addresses can be faked. That's called spoofing, and the number could correspond to somebody else -- which is why some seventy-year-old grandma may get a letter saying, 'You downloaded porn.'

Of course, many people swept up in such cyber-dragnets actually did download the movie in question, and that makes them even more susceptible to coercion, Kerr believes. "Let's say you're living in the suburbs and your wife opens the letter and says, 'Why did you download *Teen Anal Nightmare 6*?'

"These letters are like invoices. You send out 1,000 letters, and half the people freak out and pay you -- and if they each pay you \$5,000, it doesn't take an idiot to figure out that could be pretty profitable pretty quick. You could take a small, pornographic movie made for tens of thousands of dollars and potentially turn it into millions."



Kerr concedes that porn companies are entitled to copyright protection, too -- "but the question becomes, is this sort of legal mechanism the right way to enforce it, since it's so grossly unfair and there's so much potential to get the wrong people."



If such innocents refused to pay off, they're unlikely to be dragged before a judge. Kerr says actually litigating such matters is expensive, cutting into the model's profits. But the prospect of being an exception to this rule can scare people into capitulating. "One of my clients was a third-grade teacher who didn't even know how to download a movie," he recalls. "But she said, 'If I get accused of downloading this movie, it's going to make me look like a pedophile and I'm going to get fired. So I'll cough up a few thousand dollars to make it go away.'"

Saunders doesn't share particulars about her current client -- identified as John Doe 21 -- and the only detail contained in the motion is the name of the movie allegedly downloaded illegally: *Gangbanger*. However, she feels her filing will help move the judiciary to pour cold water on the practice.

"The majority of jurisdictions across the U.S. have dealt with these types of cases, but there is little continuity between the courts' decisions," she concedes. "For instance, the District Court in Northern California and Washington D.C. reflect both ends of the spectrum. The Court in Northern California has come down with recent rulings that are incredibly favorable to defendants. The District Court in Washington

D.C., however, is a whole different story, and recent rulings reflect D.C as a place unwilling to even entertain legitimate arguments sets forth by defendants, at least until later stages of litigation.

"Colorado has yet to hear these types of cases, however, which makes it difficult, if not impossible, to accurately predict what side the court will come down on her," she concedes. "Patrick Collins Inc. v. Does 1-26 is really the first to test the waters on how the federal court in Colorado will treat these cases. As a case that will undoubtedly set precedent, I believe that there's a huge significance in successfully fighting the suit. A ruling for the plaintiff could open the doors for an increasing flood of litigation of this type in Colorado; whereas, a ruling for defendants would largely discourage these unfortunate lawsuits."

Her bottom line? "As the next few months progress, it is my hope that the court sees the case for what

EXHIBIT B

SFGate.com
Back to Article
SFGate.com

Print This Article

advertisement | your ad here

Steele Hansmeier drops suit against 'porn granny'

James Temple
Wednesday, August 31, 2011

-- Technology remains the undisputed driving force behind job creation and office leasing in San Francisco.

Yelp, LinkedIn, Salesforce.com, Dolby Laboratories and Advent Software are all hunting for more space in the city, industry sources say. Meanwhile, Mayor Ed Lee announced expansion plans for both Autodesk and Zendesk this week.

Tech firms moving to or expanding within San Francisco almost universally cite the local workforce. The creative and highly trained engineers they want to employ want to live in the city - or at least be able to commute to their jobs easily from surrounding areas.

In all, about 85 technology firms are scouting the local market for around 2.7 million square feet of office space, according to an analysis by real estate brokerage Jones Lang LaSalle. Through the first seven months of the year, the industry leased 4 million square feet in the city - 1.2 million of which represented growth (many of the leases were renewals for existing firms). Companies in the sector fill about 15 percent of the city's occupied office space but now represent about 30 percent of the growth.

"The trend is clear," said Colin Yasukochi, director of research at Jones Lang LaSalle. "They are growing at a substantially faster rate than any other industry in the market."

On Tuesday, Lee announced the official opening of Zendesk in the Mid-Market district while revealing that the customer-support software company sealed a deal to double its planned space there to 35,000 square feet. Opening the office at 989 Market St. makes Zendesk the first company to take advantage of the payroll tax exclusion passed in April.

The controversial measure backed by Lee was designed to help revitalize the rundown district by luring technology companies, particularly those keen to avoid what ends up being a steep tax amid an initial public offering. It was mainly driven by Twitter, which had been threatening to move its headquarters out of the city but ultimately signed a lease at the Market Square building.



Click Here

"Our administration has pushed very hard this concept that technology companies should start here, grow here and stay here," Lee said in an interview. "It's a huge engine in our local economy."

On Monday, Lee also said Autodesk, a leading engineering software company, will expand its space at One Market Plaza by another 36,000 square feet. That marks the San Rafael company's second expansion in the past six months, bringing its total San Francisco presence to 150,000 square feet.

About 500 of Autodesk's workers are now located in the city, a number it expects will reach 700 within the next three to five years.

The latest lease "is about investing in our future and investing in this creative and innovative city," Autodesk chief executive Carl Bass said in a statement. "With our offices in the heart of downtown, we see our expansion playing an important role in attracting the best talent from around the Bay Area."

"Porn granny" update: A Chicago law firm has dropped its claims against an East Bay grandmother whom it accused of illegally downloading pornography, in a case that some observers said bordered on extortion.

"It is such good news as this lawsuit has been hanging over my head," said Jane, a retired widow in her 70s who asked that her real name not be used. "But at the same time, there's a certain bitterness about the whole thing."

We first reported on the suit in July, noting that Steele Hansmeier PLLC had filed cases on behalf of adult entertainment companies against thousands of people around the country. The suits usually seek damages for what the law firm says are illegal downloads of adult entertainment on personal computers.

In letters to defendants, the law firm strongly urges people to settle for a few thousands dollars, reminding them that it's less than what they'd probably pay in attorney's fees and that a settlement would keep their name out of a court case tied to porn.

Legal observers such as the Electronic Frontier Foundation say that the embarrassing allegations and low fees can compel people to pay up even if they've done nothing wrong.

Media companies and law firms can dig up defendant names by subpoenaing Internet service providers for the account holders linked to the online address seen downloading or sharing copyrighted files on sites such as BitTorrent. But it's a notoriously fallible way to identify actual violators. Internet customers routinely allow friends and family to use their

accounts or inadvertently leave their Wi-Fi open to neighbors or passers-by.

Jane doesn't know how her account was used for these purposes, but insists she never downloaded pornography and had never heard of BitTorrent. She refused to pay the settlement fee.

In a recent letter, Steele Hansmeier said it wasn't pursuing further action against her. It mentioned The Chronicle column but suggested the decision had nothing to do with publicity or principle. Rather, it says the law firm found the actual person responsible for downloading the material in question.

Jane finds the claim dubious.

"They had an unwinnable case, and I called them on it," she said. "And I hope other people do, too."

Law firm partner John Steele didn't respond to an inquiry.

If the firm did find the "real" criminal, one might think it would - or at least should - offer an apology for the strain the case placed on an elderly woman. No such luck.

Instead, in a snide aside, the letter underscored that the firm knew she talked to the newspaper - but that it was impervious to such actions.

"Regarding the San Francisco article, publicity about our efforts are always welcome as it deters infringers," read the letter signed by Steele. "Also, a movie producer hired our firm after reading the article and for that I thank you."

Dot-commentary runs Wednesdays, Fridays and Sundays. Follow @jtemple on Twitter or e-mail jtemple@sfchronicle.com.

<http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/08/31/BUAC1KT44.DTL>

This article appeared on page **D - 1** of the San Francisco Chronicle

© 2011 Hearst Communications Inc. | [Privacy Policy](#) | [Feedback](#) | [RSS Feeds](#) | [FAQ](#) | [Site Index](#) | [Contact](#)

EXHIBIT C

about | services | technology | press / news | partners | contact

CURRENTLY PROTECTING 20727 COPYRIGHTS

TECHNOLOGY PROTECTING CREATIVITY

Mattel appeals \$310M award in doll copyright case <http://ft.co>

MONETIZATION

how much are you losing to copyright infringement?

It's estimated that digital piracy accounts for almost one quarter of Global Internet traffic.† CEG's premier Monetization service protects and monetizes all types of content including video, audio, images, text, software, and video games across multiple Peer-to-Peer protocols and websites.

pinpoint digital copyright infringement

Using our proprietary next-generation scanning and cutting edge digital matching technology, our Monetization service provides perpetual global monitoring of your content for copyright infringements across multiple Peer-to-Peer protocols and websites.

- Peer-to-Peer (P2P) Networks: BitTorrent, eDonkey, Gnutella, Gnutella2, Ares, Kazaa
- Websites: Corporate, Commerce, Commercial, Small Business, Ad Supported, News Conglomerates, Entertainment, Lifestyle, and more

Infringements are tracked and authenticated using a strict multi-stage process, involving automated matching and dual-human verification, effectively eliminating all false positives. Every infringing file is then traced to determine the host or Internet Service Provider (ISP). Customizable notices are automatically generated and sent directly to infringing parties or via an ISP. Infringers receive the notification directing them to Copyright Enforcement Group's branded settlement portal www.copyrightsettlements.com, where they can choose amongst multiple settlement options.

recoup revenue from digital piracy

Establish a new revenue source while offering infringers multiple settlement options with our Monetization service. Settlement offers are fully customizable and can include opportunities such as hard goods, subscriptions, licensing arrangements, straight settlements or any other offering of your choice. Your options are limitless.

Content owners can choose a soft fan-friendly marketing based approach, a stringent graduated response system, models that include litigation, leveraging CEG's vast intellectual property attorney network or anything in-between.

Our fully customizable Monetization service solution is available at no cost to content owners. Contact us for additional details.

† Price, David. "Technical Report: An Estimate of Infringing Use of the Internet". http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf. Jan 2011.

sign up for a free consultation

name

email *

phone

GET CONSULTATION

MONETIZATION

TRACKING

TAKEDOWN

BUSINESS INTELLIGENCE

SATellite

Track your copyrighted content across the globe utilizing our cutting edge technology, SATellite. [read more](#)

C4

Our secure, web-based client portal, provides real-time piracy data and statistics 24 hours a day, every day. [read more](#)

home | about | services | technology | press / news | partners | terms of use | privacy policy | contact

© 2012 Copyright Enforcement Group. All rights Reserved.

EXHIBIT D



New Anti-Piracy Solutions and Business Intelligence Services Launched by Copyright Enforcement Group (CEG)

Copyright Enforcement Group (CEG) today announced the launch of comprehensive anti-piracy solutions and in-depth business intelligence services including Infringement Monetization, Content Tracking, Content Takedown, and Business Intelligence.

Beverly Hills, CA ([PRWEB](#)) January 11, 2012 -- Copyright Enforcement Group (CEG) today announced the launch of comprehensive anti-piracy solutions and in-depth business intelligence services including Infringement Monetization, Content Tracking, Content Takedown, and Business Intelligence.

CEG's new line of fully-customizable services gives way to multiple anti-piracy solutions including a fully-customizable Monetization service solution that is available at no cost to content owners.

- **Infringement Monetization:** CEG's premier Monetization service protects and monetizes all types of content including video, audio, images, text, software, and video games across multiple Peer-to-Peer protocols and websites.
- **Content Tracking:** CEG's Data Services identify infringements and provide an invaluable, perpetual flow of raw data.
- **Content Takedown:** CEG's proprietary Takedown Notice service provides perpetual global monitoring and managed takedown notifications for copyright infringements across multiple Peer-to-Peer protocols and websites.
- **Business Intelligence:** CEG's Business Intelligence service provides the data analysis necessary to accurately interpret data and facilitate pertinent business decisions.

SATellite, CEG's proprietary platform, has centric capabilities geared towards the perpetual surveillance of multiple Peer-to-Peer protocols (P2P) and websites; it is the backbone of CEG's extensive line of anti-piracy and business intelligence solutions. The cutting edge technology enables CEG to track, monetize, and analyze all forms of copyrighted content - audio, video, image, text, video games and software - across multiple Peer-to-Peer protocols (P2P) and websites.

To learn more about CEG's Services and the SATellite Platform, please visit <http://www.ceg-intl.com>. To schedule a free consultation please call 877 5 COPYRIGHT (877 526 7974) ext 175 or email [salesteam\(at\)ceg-intl\(dot\)com](mailto:salesteam(at)ceg-intl(dot)com).

About Copyright Enforcement Group

Copyright Enforcement Group (CEG) provides first-in-class copyright protection, offering comprehensive anti-piracy solutions and in-depth business intelligence to copyright owners worldwide. Cutting edge technology enables CEG to track, monetize, and analyze all forms of copyrighted content - audio, video, image, text, video games and software - across multiple Peer-to-Peer protocols (P2P) and websites. To learn more about CEG's services, please visit <http://www.ceg-intl.com>.

###



Contact Information

PR Department

Copyright Enforcement Group

<http://www.ceg-intl.com>

877-526-7974

Online Web 2.0 Version

You can read the online version of this press release [here](#).

CERTIFICATE OF SERVICE

I hereby certify that on March 26, 2012, I served a copy of the foregoing document on:

Via mail

Mike Meier
The Copyright Law Group, PLLC
4000 Legato Road, Suite 1100
Fairfax, VA 22033
Attorney for Plaintiff

Via fax

Law Enforcement Paralegal
Charter Communications, Inc.
Fax 314-909-0609
ISP

Via fax

Subpoena Compliance
Clearwire
1475 120th Avenue NE
Bellevue, WA 98005
Fax 888-252-0563
ISP

Via fax

EarthLink Legal Dept/Subpoena Compliance
1375 Peachtree Street
Level A
Atlanta, GA 30309
Fax 404-287-4905
ISP

Via fax

Road Runner
Subpoena Compliance Team
13820 Sunrise Valley Drive
Herndon, VA 20171
Fax 704-697-4911
ISP

Via fax

Sprint Corporate Security
6480 Sprint Parkway
Overland Park, KS 66251
Fax 913-315-0736 (Alternate fax to 913-315-0735)
ISP

Via fax

Verizon Legal Compliance
Custodian of Records
P.O. Box 1001
San Angelo, TX 76902
Fax 325-949-6916
ISP

/s/ John Doe

John Doe

Pro se