J. Curtis Edmondson, CSB# 236105
15490 NW Oak Hills Drive
Beaverton, OR 97006
Phone: 503-701-9719
Fax: 503-214-8470
Email: jcedmondson@edmolaw.com

Attorney for Defendant(s) DOE.

IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF CALIFORNIA

CP PRODUCTIONS, INC.,	Case No.: 2:12-CV-00616(WBS)(JFM)
Plaintiff,	DOE's MOTION TO QUASH AND/OR FOR A PROTECTIVE ORDER
vs.	
UNKNOWN,	Hon. William B. Shubb
Defendant.	Hearing Date: July 5, 2012 Hearing Time: 2pm
	ORAL ARGUMENT REQUESTED

TO ALL COUNSEL AND THEIR ATTORNEY'S OF RECORD:

Pursuant to the Federal Rules of Civil Procedure and the inherent power of this Court, located at the Sacramento Division of the Eastern District of California, in front of Hon. Judge William B. Shubb or Magistrate Judge John F. Moulds, Defendant DOE does hereby move that this Court quash the subpoena served on Charter Communications to those Defendants that lie outside the Eastern District of California and to issue a protective order preventing demand letters from being sent to the defendants listed on Exhibit B of plaintiff's Complaint.

This motion will be based on this notice, the relevant statutes, and the argument presented herein.

ISSUES PRESENTED

1. Should this Court quash the subpoenas for the BitTorrent addresses that lie outside this Judicial District?

2. Should this Court issue a protective order so that the defendants may proceed as "DOES" until judgment is entered?

3. Should this Court issue a protective order so that the personal information of the alleged "co-conspirators" of defendant is not turned over to plaintiff until defendant's liability has been established?

INTRODUCTION

This case is about the unfortunate intersection of internet copyright infringement, pornography, and an economic business model. On one hand, CP Productions, Inc. complains that the DOE has caused them economic damage. On the other hand, the DOE, once named, will be publicly connected to the pornography industry. This is of no concern to CP Productions, Inc. which is their course in trade. To the DOE, it is a modern day version of Hawthorne's "The Scarlet Letter".

At issue is the file-sharing program "BitTorrent". BitTorrent is a content neutral file distribution program. See http://www.bittorrent.com/company/about. BitTorrent is remarkably efficient at transferring large files, whether infringing or not. BitTorrent is efficient because it is a bit like the "Star Trek" transporter – disassembling parts of the file at the source and

reassembling them at the destination. Each smaller piece is transported by a "node computer". A good discussion of the technology can be found at:

http://computer.howstuffworks.com/bittorrent.htm .

For CP Productions, Inc. to bring a claim against DOE for infringement, it must first identify the "seed" file linked to the infringed work. Then CP Productions, Inc. must install a piece of software that "monitors" the transfer of data in the internet to determine the IP address of the "seed file" that was used by DOE. Then CP Productions, Inc. collects the IP addresses and determines where DOE is located using "geolocation" software. Complaint, Ex B.

The business side of this case involves the use of mass joinder and the threat of litigation to extract settlements (typically $2-3K). Mass joinder to make money is not a new concept in California. The Trevor Law Group used a similar technique to extract settlements at the beginning of this century. *People ex rel. Lockyer v. Brar*, 115 Cal. App. 4th 1315, 1316-1317 (Cal. App. 2004); see also *Molski v. Mandarin Touch Restaurant*, 347 F. Supp. 2d 860, 867 (C.D. Cal., 2004).

From reading plaintiff's Complaint, however, it is not entirely clear whether CP Productions is suing all of the individuals associated with the IP addresses CP Productions lists on Exhibit B of its Complaint as co-conspirators to the alleged infringement or whether they are only suing a single John Doe defendant. To cover both possibilities, this Motion to Quash argues both improper joinder (if multiple defendants are being sued) as well as for a protective order to prevent the ISPs listed in Exhibit B of plaintiff's Complaint from disclosing to plaintiff the contact information for any of the individuals associated with the IP addresses in Exhibit B of plaintiff's Complaint until liability on the part of the Defendant (if only one defendant is being sued).

Furthermore, CP Productions, Inc.'s Complaint fails to plead what specific technology is used to determine if that specific IP address is infringing. For example, the Piatek article illustrates the problem of false positives. (This article is provided for the Court's reference and review).

1. The Court should quash subpoenas for IP addresses that lie outside this judicial district in the interests of judicial economy.

This Court has the discretion to quash subpoenas that would disclose confidential information. Fed. R. Civ. P. 45(c)(3)(B). Further, Fed. R. Civ. P. 26(c)(1) allows a protective order to issue that protects a person from annoyance, embarrassment, oppression, or undue burden or expense. Fed. R. Civ. P. 20(a) allows for permissive joinder, but failure to join all parties does not result in a jurisdictional defect. *Coleman v. Quaker Oats Company*, 232 F.3d 1271, 1296 (9th Cir. 2000).

Additionally, requests for pseudonymity have been granted when anonymity is necessary to preserve privacy in a matter of a sensitive and highly personal nature. See *Does I Thru XXIII v. Advanced Textile Corp.*, 214 F.3d 1058, 1068 (9th Cir. 2000). An allegation that an individual illegally downloaded adult entertainment likely goes to matters of a sensitive and highly personal nature.

Joinder fails to promote trial convenience and expedition of the ultimate determination of the substantive issues in this case. See *Pac. Century Int'l*, 2011 U.S. Dist. LEXIS 124518, 2011 WL 5117424, at *3 (describing the "logistical nightmare" of joining 101 Doe defendants in such an action). Though the 590 Doe defendants may have engaged in similar behavior, they are

likely to present different defenses. See *BMG Music v. Does 1-203*, No. Civ. A. 04-650, 2004 U.S. Dist. LEXIS 8457, 2004 WL 953888, at *1 (E.D. Pa. Apr. 2, 2004). As one court noted, "Comcast subscriber John Doe 1 could be an innocent parent whose internet access was abused by her minor child, while Jon 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." *Id.*

Other courts have found misjoinder in similar copyright infringement cases. See, e.g., *Pac. Century Int'l, Ltd. v. Does 1-101*, No C 11-02533 DMR, 2011 U.S. Dist. LEXIS 124518, 2011 WL 5117424, at *3 (N.D. Cal. Oct. 27, 2011)[1]. These courts have found allegations that BitTorrent users downloaded the same copyrighted files were insufficient to support mass joinder.

It is not unclear from Plaintiff's pleadings why discovery is needed on the defendants' identities unless it is to send threatening letters indicating that defendants are liable for infringement. Assuming this is true, it is clear from the Plaintiff's own pleadings that the majority of the purported defendants or third parties may live hundreds of miles from this courtroom. For example, the online geolocation software (http://www.ipligence.com/geolocation) demonstrates that the first five IP addresses are from:

IP Address #	City	Court Jurisdiction
108.0.161.125	Cerritos	CD Cal
108.0.190.107	Walnut	CD Cal
108.0.218.138	Long Beach	CD Cal

[1] See also: *Diabolic Video Prods. v. Does 1-2099,* No. C 10-5865 PSG, 2011 U.S. Dist. LEXIS 58351, at *9 (N.D. Cal. May 31, 2011);
Pac. Century Int'l, Ltd. v. Does 1-101, No C 11-02533 DMR, 2011 U.S. Dist. LEXIS 73837, 2011 WL 2690142, at *2-*4 (N.D. Cal. Jul. 8, 2011);
IO Group, Inc. v. Does 1-435, No. C 10-4382 SI, 2011 U.S. Dist. LEXIS 14123, 2011 WL 445043, at *3-*6 (N.D. Cal. Feb. 3, 2011);
On The Cheap, LLC v. Does 1-5011, No. C 10-4472 BZ, 2011 U.S. Dist. LEXIS 99831, 2011 WL 4018258, at *2 (N.D. Cal. Sept. 6, 2011)

108.0.220.152	Long Beach	CD Cal
108.13.3.56	Huntington Beach	CD Cal

* These IP addresses were rechecked with "Infosniper".

Not one of the above IP addresses points to Eastern District of California, a fact that plaintiff could easily have learned prior to filing their complaint. Given that plaintiff was able to use geolocation technology to determine that the Unknown Defendant lives specifically in Sacramento, CA (see Complaint, Exhibit A), it is curious that plaintiff did not use that same technology to determine the city (and hence the jurisdiction) of the alleged co-conspiritors (Exhibit B). In any case, it is clear that CP Productions, Inc. is asking this Court to draw in defendants from all over the state of California for this matter. This court should, in the very least, only allow CP Productions, Inc. to proceed on defendants that are within this judicial district.

2. Defendants should not be allowed to threaten DOE defendants with litigation unless the Complaint is amended or DOEs are joined.

"[U]nder Rule 26(c), the Court may *sua ponte* grant a protective order for good cause shown." *McCoy v. Southwest Airlines Co., Inc.*, 211 F.R.D. 381, 385 (C.D. Cal. 2002). The Court issues the limited protective order described below because the ISP subscribers may be innocent third parties, the subject matter of the suit deals with sensitive and personal matters, and the jurisdictional and procedural complications might otherwise dissuade innocent third parties from contesting the allegations.

Here, as has been previously discussed by other courts in this district, the ISP subscribers may not be the individuals who infringed CP Productions, Inc.'s copyright. *See*, e.g., *Pac. Century Int'l*, 2011 U.S. Dist. LEXIS 124518, 2011 WL 5117424, at *2; *see also IO Group, Inc. v. Does 1 19*, No. C 10 03851 SI, 2011 WL 772909, at *1 (N.D. Cal. Mar. 1, 2011) (granting the plaintiff additional time to identify and serve the true defendant where a subscriber asserted that he did not infringe plaintiff's work, suggesting that someone else used his IP address to infringe the plaintiff's work, and the plaintiff claimed that it needed to take third-party discovery from the subscriber to try to identify who actually used the subscriber's IP address to allegedly infringe the plaintiff's work).

Clearly, the privacy interests of innocent third parties weighs heavily against the public's interest in access to court documents. *See Gardner v. Newsday, Inc.*, 895 F.2d 74, 79-80 (2d Cir. 1990).

A protective order is an equitable and fair way to allow CP Productions, Inc. to litigate their rights and for potentially innocent third parties to not have their names sullied as potential defendants. Therefore, Plaintiff should not be permitted to access their contact information or send them threatening letters demanding settlement.

3. Plaintiffs should not require the ISPs to turn over the personal information of the nonparties in this case until the Defendant's liability has been determined or until the nonparties have been directly charged under some theory of liability.

If the individuals associated with the IP addresses listed on Exhibit B of plaintiff's Complaint are nonparties to this case, CP Productions has no legitimate need for their contact information to pursue its copyright infringement claim against Unknown Defendant, especially given that Unknown Defendant's liability has not yet been established at this time.

Furthermore, allowing plaintiff access to the nonparties' contact information will make those nonparties vulnerable to loss of reputation as well as plaintiff's shakedown tactics even though they have not been charged in any fashion under any theory of liability.

Here, Plaintiff's counsel, via phone conversation, stated that the parties on Exhibit B of Plaintiff's Complaint are not liable for infringement. Therefore, they should not receive letters threatening them with copyright infringement and requesting settlement in the amount ranging from $3,000 to $4,000.

Conclusion

Given the nature and types of these cases, the Court should be extra diligent in protecting the identities of the defendants. Therefore DOE respectfully requests that this Court quash the subpoena for all members who live outside this judicial district and issue a protective order so that their true identities are not produced until a final judgment is entered against them.

/x/ J. Curtis Edmondson

May 24, 2012

Declaration of J. Curtis Edmondson in the Motion to Quash

I, J. Curtis Edmondson, declare this to be true under penalty of perjury, pursuant to 28 U.S.C. 1746 on the date set forth at my signature below:

1. I am an attorney licensed to practice in the State of California and have been admitted to the bar of the Eastern District of California. I am counsel of record in this matter.
2. I represent a number of defendants who reside outside this judicial district. These defendants are collectively named "DOE" to prevent their names being associated with pornography.
3. In this brief, I used two internet based software programs to determine the "geolocation" of the first five IP addresses in the complaint.
4. My background is in electrical engineering and I am a member of the patent bar. I believe I am competent to testify on my use of the aforementioned geolocation programs and to testify about computer technologies (BitTorrent) in general.
5. On May 24th, I called and spoke with Brett L. Gibbs about this case. I asked him if the parties on Exhibit "B" of the Complaint are considered liable for copyright infringement. He said they were not.

I declare under penalty of perjury under the laws of the state of California that the foregoing is true and correct.

Executed this 24th day of May, 2012, at Beaverton, Oregon.

/x/ J. Curtis Edmondson

Declarant

Declaration of William Petillo in the Motion to Quash

I, William Petillo, declare this to be true under penalty of perjury, pursuant to 28 U.S.C. 1746 on the date set forth at my signature below:

1. I am currently enrolled in the Paralegal Program at Portland Community College. I have been working as an office assistant for J. Curtis Edmondson since August 2011.
2. On May 23, 2012, in the process of assisting J. Curtis Edmondson in preparing this brief, I entered the first five IP addresses listed on Exhibit B of plaintiff's Complaint into www.infosniper.net, a website that provides free geolocation. The results of these searches are included in this Motion.
3. On May 24, 2012, at approximately 10:45am and over the course of about 10 minutes, I overheard a telephone conversation between J. Curtis Edmondson and Brett L. Gibbs. Although I could only hear what J. Curtis Edmondson was saying, it was obvious from context that Brett L. Gibbs had expressed that the individuals associated with the IP addresses listed in Exhibit B of plaintiff's Complaint are not parties to this case.

I declare under penalty of perjury under the laws of the state of California that the foregoing is true and correct.

Executed this 24th day of May, 2012, at Beaverton, Oregon.

/x/ William Petillo

Declarant

PROOF OF SERVICE

I hereby certify that on May 24, 2012, a copy of the foregoing was filed by CM/ECF with the Civil Clerk at the Eastern District of California.

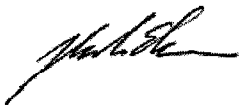
The following will receive a copy of the foregoing by electronic copy:

Motion to Quash

Brett L. Gibbs, Esq.
Prenda Law, Inc.
38 Miller Avenue, #263
Mill Valley, CA 94941
415-325-5900
blgibbs@wefightpiracy.com

Dated: 5/24/2012

Respectfully Submitted,



J. Curtis Edmondson
Law Offices of J. Curtis Edmondson
15490 NW Oak Hills Drive
Beaverton, OR 97006
(503) 701-9719 ph
(503) 214-8470 fax
Attorney for Defendant DOE

EXHIBIT A

Challenges and Directions for Monitoring P2P File Sharing Networks – or – Why My Printer Received a DMCA Takedown Notice

Michael Piatek* Tadayoshi Kohno * Arvind Krishnamurthy*

Abstract— We reverse engineer copyright enforcement in the popular BitTorrent file sharing network and find that a common approach for identifying infringing users is not conclusive. We describe simple techniques for implicating arbitrary network endpoints in illegal content sharing and demonstrate the effectiveness of these techniques experimentally, attracting real DMCA complaints for nonsense devices, e.g., IP printers and a wireless access point. We then step back and evaluate the challenges and possible future directions for pervasive monitoring in P2P file sharing networks.

1 Introduction

Users exchange content via peer-to-peer (P2P) file sharing networks for many reasons, ranging from the legal exchange of open source Linux distributions to the illegal exchange of copyrighted songs, movies, TV shows, software, and books. The latter activities, however, are perceived as a threat to the business models of the copyright holders [1].

To protect their content, copyright holders police P2P networks by monitoring P2P objects and sharing behavior, collecting evidence of infringement, and then issuing to an infringing user a so-called *Digital Millennium Copyright Act (DMCA) takedown notice*. These notices are formal requests to stop sharing particular data and are typically sent to the ISPs corresponding to the IP addresses of allegedly infringing users.

The combination of large-scale monitoring of P2P networks and the resulting DMCA complaints has created a tension between P2P users and enforcement agencies. Initially, P2P designs were largely managed systems that centralized key features while externalizing distribution costs, e.g., Napster's reliance on a centralized index of pointers to users with particular files. Legal challenges to these early networks were directed towards the singular organization managing the system. In contrast to these managed *systems*, currently popular P2P networks such as Gnutella and BitTorrent are decentralized *protocols* that do not depend on any single organization to manage their operation. For these networks, legal enforcement requires arbitrating disputes between copyright holders and P2P users directly.

*Dept. of Computer Science and Engineering, Univ. of Washington. E-mails: piatek@cs.washington.edu, yoshi@cs.washington.edu, arvind@cs.washington.edu. Additional information about this paper is available at http://dmca.cs.washington.edu/.

The focus of this paper is to examine the tension between P2P users and enforcement agencies and the challenges raised by an escalating arms race between them. We ground this work in an experimental analysis of the methods by which copyright holders currently monitor the BitTorrent file sharing network. Our work is based on measurements of tens of thousands of BitTorrent objects. A unique feature of our approach is that we intentionally try to receive DMCA takedown notices, and we use these notices to drive our analysis.

Our experiments uncover two principal findings:

- Copyright holders utilize inconclusive methods for identifying infringing BitTorrent users. We were able to generate hundreds of DMCA takedown notices for machines under our control at the University of Washington that were not downloading or sharing any content.
- We also find strong evidence to suggest that current monitoring agents are highly distinguishable from regular users in the BitTorrent P2P network. Our results imply that automatic and fine-grained detection of monitoring agents is feasible, suggesting further challenges for monitoring organizations in the future.

These results have numerous implications. To sample our results, based on the inconclusive nature of the current monitoring methods, we 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 network.

Based on these observations, we then explore how the arms race between content consumers and monitoring organizations might evolve and what challenges would arise for both parties. We explicitly do not take sides in this arms race. Rather, we take special care to be independent and instead consider methods by which both users and monitoring organizations could advance their interests. Our goal is to provide a foundation for understanding and addressing this arms race from both perspectives. While couched in the context of the sharing of copyrighted content, we also believe that our results and directions will become more broadly applicable as new uses for P2P file sharing networks evolve.

	Complaint type						Totals	
Trace	Movie	Music	Television	Software	Books	Mixed	Complaints	Swarms obs.
August, 2007	82	0	11	18	11	0	122	55,523
May, 2008	200	0	17	46	0	18	281	27,545

Table 1: DMCA takedown notices received during our BitTorrent experiments. All are false positives.

2 Background

BitTorrent overview: BitTorrent is a P2P file distribution tool designed to replace large file downloads over HTTP. Rather than downloading a large file directly, a BitTorrent user instead downloads a small torrent file which contains metadata regarding the original file(s), e.g., names and sizes, as well as the address of a coordinating *tracker* for the swarm. The tracker is a rendezvous service for peers in a particular swarm, providing a random set of active downloaders upon request. New users register with the tracker, advertising their status as a potential peer, and connect to the set of peers returned by the tracker to begin exchanging data. BitTorrent peers distribute small blocks that comprise the original file. Ideally, a user with a complete copy of the file need only send each block to a few peers and the rest of the distribution will be performed by the swarm.

DMCA Enforcement: At present, DMCA takedown notices are the principle mechanism used for enforcing copyright on the Internet in the United States. DMCA notices are sent to ISPs when monitoring agencies detect alleged infringement. Separate and less frequently used mechanisms are actual legal prosecutions and "pre-settlement" letters that inform users of plans for prosecution if a settlement payment is not made. To date, we have not received any pre-settlement letters as a result of our experiments.

Takedown notices generally include the date and time of an observation, metadata for the infringing file, and the IP address of the infringing host. Network operators then respond to the complaint, often forwarding it (if possible) to the user identified by the network information.

A key question for understanding the enforcement process is: how are infringing users identified? We consider two options for detection in BitTorrent:

- *Indirect detection* of infringing users relies on the set of peers returned by the coordinating tracker only, treating this list as authoritative as to whether or not IPs are actually exchanging data within the swarm.
- *Direct detection* involves connecting to a peer reported by the tracker and then exchanging data with that peer. Direct detection has relatively high resource requirements, a topic we revisit in Section 6.

While direct detection is more conclusive and is the stated approach for monitoring the Gnutella P2P network by at least one content enforcement agency [11], we find that many enforcement agencies instead use indirect detection when monitoring BitTorrent.

3 Data Sources and Methodology

Our understanding of copyright enforcement in BitTorrent is based on measurement and analysis of tens of thousands of live BitTorrent swarms and the DMCA complaints these measurements attracted. To gather a set of candidate swarms to monitor, we continuously crawled popular websites that aggregate torrent metadata. For each observed swarm, our instrumented BitTorrent clients contacted the associated tracker, requesting a set of bootstrapping peers. These requests were repeated for each swarm every 15 minutes from 13 vantage points at the University of Washington. Crucially, querying the tracker for a set of bootstrapping peers allowed us to determine membership in swarms and advertise our presence as a potential replica *without uploading or downloading any file data whatsoever.*

The process of collecting these traces generated many DMCA takedown notices; these are summarized in Table 1. Our initial trace (August, 2007) was collected in support of a separate measurement study of BitTorrent [9]. During this prior work, we viewed DMCA complaints as an annoyance to be avoided. More recently, the realization that we had managed to attract complaints without actually downloading or uploading any data prompted us to revisit the issue. Analyzing the complaints in more detail, we were surprised to find multiple enforcement agencies sourcing takedown notices for different content, demonstrating that spurious complaints (for machines that were not actually infringing) were not isolated to a single agency (or industry).

In May, 2008, we conducted a new measurement study of BitTorrent aimed at answering two questions. First, *has the enforcement approach changed?* We find that it has not; we continue to receive DMCA complaints even in the absence of data sharing. Our second question is: *can a malicious user falsely implicate a third party in copyright infringement?* We find that framing is possible given the monitors' current use of indirect detection of infringing users, a topic we discuss next.

4 False Positives with Indirect Detection

The main weakness in current methods of detecting copyright infringement in BitTorrent appears to be the treatment of indirect reports as conclusive evidence of

Host type	Number of complaints
Desktop machine (1)	5
IP Printers (3)	9
Wireless AP (1)	4

Table 2: False positives for framed addresses.

participation. We now describe how the use of indirect reports exposes monitoring agents and innocent users to attacks from malicious users attempting to implicate others. We verify one variant of this family of attacks experimentally and quantify its effectiveness in the wild.

4.1 The Misreporting Client Attack

The first request from a BitTorrent client to a tracker serves two purposes. First, it elicits a response that provides the newly joined client with an initial set of peers with which to exchange data. Second, the request notifies the tracker that a new peer is available and can be listed in responses to future requests. By default, BitTorrent trackers record the source IP address from the request as the actual address of the peer to be delivered to others. But, some BitTorrent tracker implementations support an optional extension to the peer request message that allows requesting clients to specify a different IP address that the tracker should record in its list of peers instead. This is intended to provide support for proxy servers and peers/trackers behind the same NAT. But, when combined with the lack of verification of tracker responses by monitoring agents, this extension also allows malicious clients to frame arbitrary IPs for infringement via a simple HTTP request. We refer to this behavior as the misreporting client attack. A sample HTTP request to frame a target IP address A.B.C.D, after standard parsing of the relevant torrent metadata, is as follows:

```
wget 'http://torrentstorage.com/announce.php
?info_hash=%0E%B0c%A4B%24%28%86%9F%3B%D2%CC%
BD%0A%D1%A7%BE%83%10v&peer_id=-AZ2504-tUaIhr
rphVcq&port=55746&uploaded=0&downloaded=0&le
ft=366039040&event=started&numwant=50&no_pee
r_id=1&compact=1&ip=A.B.C.D&key=NfBFoSCo'
```

We designed our May, 2008 experiments to examine the effectiveness of this attack in the wild today. For each tracker request issued by our instrumented clients, we included the option for manually specifying a client IP to frame, drawing this IP randomly from a pool of IPs at the University of Washington. Each framed IP was under our direct control and none were engaged in any infringing activity. These addresses include printers, a wireless access point, and an ordinary desktop machine. As a consequence of our spoofed requests, all of these devices attracted complaints (as summarized in Table 2). We also attempted to frame two IP addresses for which no machines were associated; these IP addresses were not remotely pingable and we did not receive any complaints for these IP addresses.

Although successful, the yield of misreporting client attack is low. Of the 281 complaints generated by our May, 2008 trace, just 18 of these were for IPs that we were attempting to implicate. The remaining majority were targeted at the IP addresses from which we launched our spoofed requests. Yield was low with our initial experiments because we did not know *a priori* which trackers support the protocol extension required for IP spoofing. Those that do not simply disregard that portion of the request message and instead record the IP source address of the request message. Thus, the effectiveness of the vanilla misreporting client attack, as described above, depends on what fraction of swarms can be spoofed.

We can compute this fraction using our measurements. In addition to implicating IPs continuously, we also record swarm membership continuously. Because we know that our framed IPs did not participate in BitTorrent swarms, observing *any* framed IP in the set of peers returned by a tracker indicates that the given tracker (and swarm) support spoofed addresses. Over the duration of our trace, we observed our framed IPs in 5.2% of all swarms, suggesting that the limited yield of the misreporting client attack is simply the result of a small fraction of swarms supporting spoofing as opposed to any sanity checks that might detect spoofed IPs.

More sophisticated variants of our attacks could route the HTTP requests through a proxy or anonymization service like Tor, and could also target only those trackers that support spoofed addresses.

4.2 Additional sources of false positives

Our experiments confirm that a malicious user can implicate arbitrary IPs in illegal sharing today. But, the misreporting client attack is not the only source of false positives possible given the current approach to enforcement.

Misreporting by trackers: The most straightforward way to falsely implicate an IP address in infringement is for the coordinating tracker to simply return that IP address as a peer regardless of participation. Since the torrent metadata files that specify trackers are user-generated, a malicious user can frame arbitrary IPs simply by naming his own misreporting tracker during the creation of the torrent and then uploading that torrent to one of the many public aggregation websites that we (and enforcement agencies, presumably) crawl. From the perspective of users downloading the file, such a malicious tracker would seem no different than any other.

Mistimed reports: A tracker need not be malicious to falsely implicate users. Consider the following scenario. Bob participates in an infringing BitTorrent swarm from a laptop via WiFi with an IP address assigned via DHCP, e.g., at a university or coffee shop. Bob then closes his laptop to leave, suspending his BitTorrent client with-

out an orderly notification to the tracker that he has left. Some time later, Alice joins the same WiFi network and, due to the DHCP timeout of Bob's IP, Alice receives Bob's former address. Simultaneously, a monitoring agent queries the tracker for the swarm Bob was downloading and the tracker reports Bob's former IP. The monitoring agent then dispatches a DMCA notice to the ISP running the WiFi network naming Bob's IP but with a timestamp that would attribute that IP to Alice, a false positive. Whether this is a problem in practice depends on the relative timeouts of BitTorrent trackers and DHCP leases, neither of which is fixed. In a university environment in 2007, DHCP lease times were set to 30 minutes [4]. The interarrival time of tracker requests is typically 15 minutes at least, meaning that even a conservative tracker timeout policy of two missed requests coupled with a 30 minute DHCP lease time could result in this type of misidentification.

Man-in-the-middle: Because BitTorrent tracker responses are not encrypted, man-in-the-middle attacks at the network level are straightforward. Anyone on the path between tracker and a monitoring agent can alter the tracker's response, implicating arbitrary IPs. Further, man-in-the-middle attacks are also possible at the overlay level. For redundancy, current BitTorrent clients support additional methods of gathering peers beyond tracker requests. These include peer gossip and distributed hash table (DHT) lookup [3]. Although we have not determined experimentally if these sources of peers are used by monitoring agents, each permits man-in-the-middle attacks. DHT nodes can ignore routing requests and return false IPs in fraudulent result messages. Similarly, peers can gossip arbitrary IPs to their neighbors.

Malware and open access points: There are other ways in which innocent users may be implicated for copyright infringement. For example, their computer might be running malware that downloads or hosts copyrighted content, or their home network might have an open wireless access point that someone else uses to share copyrighted content. We do not consider these further in this paper since, in these cases, the user's IP address is involved in the sharing of copyrighted content (even if the user is innocent). Our previous examples show how it is possible for a user's IP address to be incorrectly accused of copyright violation even if no computer using that IP address is sharing copyrighted content at the time of observation.

5 False Negatives with Direct Detection

A common method employed by privacy conscious users to avoid systematic monitoring is IP blacklists. These lists include the addresses of suspected monitoring agents and blacklisting software inhibits communication to and from any peers within these address ranges. The popularity of blacklists is, in retrospect, perhaps a bit surprising given our discovery (Section 4) that monitoring agents are issuing DMCA takedown notices to IP addresses without ever exchanging data with those IPs. Nevertheless, blacklists—if populated correctly—might be effective in protecting against direct monitoring techniques that involve actual data exchange between monitoring agents and P2P clients.

Since we expect that enforcement agencies will soon shift to more conclusive methods of identifying users, we revisit the issue of blacklists and ask: if enforcement depended on direct observation, are current blacklists likely to inhibit monitoring? We find that the answer to this question is likely no; current IP blacklists do not cover many suspicious BitTorrent peers. In this section, we describe the trace analysis supporting this conclusion.

In considering which peers are likely monitoring agents and which are normal BitTorrent users, our main hypothesis is that current monitoring agents are crawling the network using methods similar to our own; i.e., crawling popular aggregation sites and querying trackers for peers. On our part, this behavior results in our measurement nodes appearing as disproportionately popular peers in our trace, and systematic monitoring agents are likely to exhibit similarly disproportionate popularity.

To test this, we first define our criteria for deciding whether or not a peer is likely to be monitoring agent, beginning by considering the popularity of peers observed in our trace on a single day (May 17th, 2008). Of the 1.1 million reported peers in 2,866 observed swarms, 80% of peers occur in only one swarm each. Of the remaining 20% that occur in multiple swarms, just 0.2% (including our measurement nodes and framed IPs) occur in 10 or more swarms. The disproportionate popularity of this small minority suggests the potential for measurement agents, but manual spot-checks of several of these IPs suggests that many are ordinary peers; i.e., they come from addresses allocated to residential broadband providers and respond to BitTorrent connection requests.

Other addresses, however, come from regions allocated to ASes that do not provide residential broadband, e.g., co-location companies that serve business customers only. Further, in several instances multiple addresses from the /24 prefixes of these organizations are among the most popular IPs and none of the addresses respond to BitTorrent connection requests. We take this as a strong signal that these are likely monitoring agents and consider any /24 prefix with six or more hosts listed in ten or more swarms to be suspicious. We manually inspected the organization information for these IPs (using whois lookup), eliminating any ASes that provide residential service. Although these ASes may host monitoring agents, we adopt a conservative standard by discarding them. This further pruning resulted in a set of 17

suspicious prefixes.

To test our list of suspicious prefixes against blacklists, we obtained the latest versions of blacklists used by the popular privacy protection software SafePeer and PeerGuardian. Of the 17 suspicious prefixes, 10 were blocked, and 8 of these, while allocated to a co-location service provider, are attributed in the blacklists to either MediaSentry or MediaDefender, copyright enforcement companies. However, seven of our suspicious prefixes (accounting for dozens of monitoring hosts) are not covered by current lists.

Repeating this analysis for additional days of our trace yields similar results, suggesting that existing blacklists might not be sufficient to help privacy conscious peers escape detection (possibly because these blacklists are manually maintained). On the other hand, our analysis also implies monitoring agents could be automatically detected by continuously monitoring swarm membership and correlating results across swarms. While the exact behavior of future monitoring peers may change, we posit that their participation in swarms will remain distinguishable. Adoption of detection techniques like ours would make it harder for monitoring agencies to police P2P networks without exposing themselves, an issue we elaborate on in the next section.

6 Lessons and Challenges

The current state of P2P monitoring and enforcement is clearly not ideal. The potential for false positives and implication of arbitrary addresses undermines the credibility of monitoring and creates a significant inconvenience for misidentified users (if not financial and/or legal penalties). We now discuss the implications of our work, considering lessons learned and likely future challenges for each of the principals involved in copyright enforcement: enforcement agencies, ISPs, and users.

6.1 Enforcement agencies

The main lesson for enforcement agencies from our work is that new methods of collecting user information are required for identification to be conclusive. A more thorough approach to detecting infringement in BitTorrent would be to adopt the stated industry practice for monitoring the Gnutella network: in the case of suspected infringement, download data directly from the suspected user and verify its contents [11]. Because we have notified several enforcement agencies of the vulnerabilities described in Section 4, we expect increasing use of direct downloads for verifying participation. This reduces the potential for false positives, but it is likely to significantly increase the cost of enforcement as well as the risk of exposing monitoring agents.

The cost of direct identification: The current monitoring approach for BitTorrent, simply issuing a tracker request, requires only a single HTTP request and response, generating at most a few kilobytes of network traffic, a single connection, and minimal processing. In contrast, directly connecting to users and downloading data would require a TCP connection apiece for each potential peer, block transfers (blocks are typically hundreds of kilobytes), and hash computations to verify data integrity.

This translates into a 10-100X increase in the throughput required for monitoring swarms. Our August, 2007 crawl, which relied primarily on tracker requests, required roughly 100 KBps of sustained throughput per measurement node to monitor roughly 55,000 swarms crawled over the course of a month. For a period of one month, direct verification of our trace would require 25 terabytes of traffic as compared to just 2.5 terabytes for indirect monitoring. Furthermore, verifying participation by directly downloading data from peers is only possible for those peers that are not masked by NATs or firewalls. Detecting those that are requires sustained operation as a server; i.e., waiting for connection requests, accepting them, and then engaging in transfers to confirm participation, further increasing the complexity and resources required for large-scale, direct monitoring.

The risk of exposing monitoring agents: A major challenge for enforcement agencies is coverage; i.e., identifying all infringing users. From the perspective of monitoring agents, achieving high coverage is straightforward; simply crawl and monitor all swarms. From the perspective of coordinating trackers, however, this behavior amounts to a denial of service attack. Many swarms are hosted on a small number of public trackers. Monitoring agents that issue frequent requests for each of the thousands of swarms that one of these public trackers coordinates are likely to be detected and blocked. Indeed, our own monitors were blocked from several of these trackers prior to rate-limiting our requests.

To avoid notice today, monitoring agents need to acquire multiple IPs in diverse regions of the address space and limit their request rate. But, IP addresses are an increasingly scarce (and expensive) resource, and monitoring more than a few swarms daily from each IP risks exposing monitoring agents through their disproportionate popularity. Given these challenges, recent calls from industry to enlist ISPs directly in enforcement are unsurprising [7]. Since ISPs do not need to participate in P2P networks to monitor user behavior, there are no apparent monitoring agents to block. The majority of complaints we have received to date reflect the tradeoff between coverage and exposure; they primarily target recently released movies, DVDs, or software packages, even though we appeared to download many more old works than new.

Challenges to direct monitoring: Even if a monitoring

agent connects directly to a device behind a given IP address, there are challenges to associating the endpoint of that communication directly to a specific physical machine, let alone a specific user. For example, suppose the IP address corresponds to a family's home cable-modem or DSL connection, and suppose the family has an open wireless access point (or an insecurely-protected access point) on their internal network. It may be challenging to determine whether the machine participating in the P2P network belongs to the family or a neighbor. To address this challenge, monitoring agents may in the future collect data about not only the IP addresses of potentially infringing parties but also operating system [8, 10, 12] and physical device [5] fingerprints.

6.2 ISPs

For ISPs, the main lesson from our work is that sanity checking is necessary to protect users from spurious complaints but not sufficient. Section 4 details several scenarios which may result in false positives that can be detected by diligent network operators. However, not all false positives can be detected, and current trends in enforcement are towards increased automation rather than increased sanity checking of complaints.

Increasing automation: Because most DMCA complaints are communicated over email, network operators typically inspect messages manually to identify users. At the University of Washington, this manual step has served as an important check that eliminates some erroneous complaints before they reach users [2].

Although having a human "in the loop" is beneficial to users, it may not be tenable with increasing rates of enforcement. While we continuously monitored tens of thousands of swarms in our traces, we garnered only hundreds of complaints, a small fraction of potentially infringing swarms. Even at this limited level of enforcement, many universities still require dedicated staff to manually process all the complaints sent to their users, increasing costs. Enforcement agencies rely on cooperation from network operators to identify infringing users, but increasing costs have pushed both ISPs and monitoring agencies towards automated enforcement.

The trend towards automation is reflected in the properties of complaints themselves. The delay between the observation of peers by enforcement agencies and the timestamp of complaint email messages has reduced significantly. The median delay for complaints generated by our trace from August, 2007 is 49 hours. For more recent complaints collected in May, 2008, the median delay is just 21 hours. Further, these recent complaints increasingly include machine readable summaries of their content, e.g., XML data with public schemas. We hypothesize that the intent is to automate the complaint process at the levels of both enforcement agency and ISP. Enforcement agencies can crawl P2P networks, generating and dispatching XML complaints which can then be parsed by ISPs and automatically forwarded to users with no human intervention.

6.3 Users

Our results show that potentially any Internet user is at risk for receiving DMCA takedown notices today. Whether a false positive sent to a user that has never even used BitTorrent or a truly infringing user that relies on incomplete IP blacklists, there is currently no way for anyone to wholly avoid the risk of complaints. But, the current approach to enforcement has a natural limiting factor. To avoid being detected, our traces suggest that enforcement agents are not monitoring most swarms and tend to target those new, popular swarms that are the most economically valuable.

In the long term, the main challenge for privacy conscious users is to develop a way to systematically detect monitoring agents. We consider two cases. If enforcement agencies continue to monitor swarms at the *protocol level* by participating in swarms, users may develop new techniques to build more dynamic, comprehensive blacklists. If ISPs are enlisted in enforcement at the *network level* by collecting traces of user traffic, we anticipate increased use of stronger encryption to frustrate realtime, automated identification of P2P protocols. We expand on each of these in turn.

Blacklists on-the-fly: Just as we expect enforcement agencies to shift from indirect to direct methods of enforcement, we also expect P2P developers to evolve IP blacklisting techniques. Currently, blacklists are centrally maintained and updated without systematic feedback from P2P users, ignoring a rich source of data: the observations of users. Many P2P networks include explicit mechanisms to identify and reward "good users"; e.g., tit-for-tat mechanisms reward contributions in BitTorrent and eDonkey. Future P2P networks may employ similar mechanisms to identify monitoring agents, gossiping this information among peers. Our traces show that the properties of monitoring agents today make this a straightforward task: they appear to share no data whatsoever, occur frequently in swarms, and are drawn from a small number of prefixes. Alternatively, sophisticated users may also try to generate honeypots (much like our own) that do not infringe or aid in copyright infringement, but that will be better able to detect (and hence dissuade) spurious DMCA takedown notices and coordinated monitoring.

Stronger encryption: Today, some BitTorrent clients include an option to use weak encryption to frustrate the traffic shaping methods used by several ISPs [6]. In the future, this encryption might be strengthened. For example, a tracker might assist two peers in establishing a

shared key in the face of ISPs that would otherwise attempt to identify and restrict P2P traffic. Such a tracker could include not only the IP addresses of participating clients, but also one-time public keys to decrease exposure to inline man-in-the-middle cryptographic attacks. To further resist monitoring, communications with trackers would have to be authenticated as well, perhaps by leveraging a lightweight, distributed PKI with popular trackers as the root authorities.

7 Conclusion

Although content providers are increasingly relying on systematic monitoring of P2P networks as a basis for deterring copyright infringement, some currently used methods of identifying infringing users are not conclusive. Through extensive measurement of tens of thousands of BitTorrent swarms and analysis of hundreds of DMCA complaints, we have shown that a malicious user can implicate arbitrary network endpoints in copyright infringement, and additional false positives may arise due to buggy software or timing effects. We have further demonstrated that IP blacklists, a standard method for avoiding systematic monitoring, are often ineffective given current identification techniques and provide only limited coverage of likely monitoring agents. These observations call for increased transparency and openness in the monitoring and enforcement process and build our understanding of current challenges and potential next steps for all parties involved in P2P file sharing: enforcement agencies, ISPs, and users.

8 Acknowledgments

We thank Ed Lazowska, Erik Lundberg, Scott Rose, Daniel Schwalbe, and Voradesh Yenbut. This work is supported by the NSF grants CNS-0720589, CNS-0722000, CNS-0722004 and by the University of Washington Department of Computer Science and Engineering.

References

[1] R. Cotton and M. L. Tobey. Comments of NBC Universal, Inc. In the Matter of Broadband Industry Practices. FCC Filing. WC Docket No. 07-52. http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6519528962.

[2] Daniel Schwalbe. Personal communication, 2008.

[3] J. Falkner, M. Piatek, J. P. John, A. Krishnamurthy, and T. Anderson. Profiling a million user DHT. In *IMC*, 2007.

[4] M. Khadilkar, N. Feamster, R. Clark, and M. Sanders. Usage-based DHCP lease time optimization. In *IMC*, 2007.

[5] T. Kohno, A. Broido, and K. Claffy. Remote physical device fingerprinting. *IEEE Transactions on Dependable and Secure Computing*, 2(2):93–108, April 2005.

[6] Message stream encryption. http://www.azureuswiki.com/index.php/Message_Stream_Encryption.

[7] MPAA wants ISP help in online piracy fight. http://news.cnet.com/8301-10784_3-9780401-7.html.

[8] Nmap - free security scanner for network exploration & security audits. http://nmap.org/.

[9] M. Piatek, T. Isdal, A. Krishnamurthy, and T. Anderson. One hop reputations for peer to peer file sharing workloads. In *NSDI*, 2008.

[10] Project details of p0f. http://freshmeat.net/projects/p0f/.

[11] C. Rampell. How it does it: The RIAA explains how it catches alleged music pirates. http://chronicle.com/free/2008/05/2821n.htm.

[12] Xprobe2. http://xprobe.sourceforge.net/.

EXHIBIT B

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

IN RE: BITTORRENT ADULT FILM COPYRIGHT INFRINGEMENT CASES

ORDER &
REPORT & RECOMMENDATION
Civil Action Nos.
11-3995(DRH)(GRB);
12-1147(JS)(GRB);
12-1150(LDW)(GRB); and
12-1154(ADS)(GRB)

----------X

APPEARANCES:

K-Beech, Inc. v. John Does 1-37, CV 11-3995 (DRH)(GRB):

For Plaintiff
Frederic R. Abramson, Esq.
160 Broadway, Suite 5000
New York, New York 10038

For Defendant John Doe #2
Joseph P. Augustine, Esq.
Augustine & Eberle LLP
90 Broad Street, Floor 25
New York, New York 10004

For Defendant John Doe #29
James Rosenzweig, Esq.
560 Fifth Avenue, 3rd Ave.
New York, New York 10036

For Defendant John Doe #35
James D. Murtha, Esq.
26 Railroad Ave. #351
Babylon, New York 11702

Malibu Media, LLC v. John Does 1-26, CV 12-1147 (JS) (GRB),
Malibu Media, LLC v. John Does 1-11, CV 12-1150 (LDW) (GRB),
Patrick Collins, Inc. v. John Does 1-9, CV 12-1154 (ADS) (GRB):

For Plaintiffs
Jason Aaron Kotzker
Kotzker Law Group
9609 S. University Blvd. #632134
Highlands Ranch, Colorado 80163

GARY R. BROWN, United States Magistrate Judge:

These actions are part of a nationwide blizzard of civil actions brought by purveyors of pornographic films alleging copyright infringement by individuals utilizing a computer protocol known as BitTorrent. The putative defendants are identified only by Internet Protocol ("IP") addresses. These four civil actions involve more than 80 John Doe defendants; these same plaintiffs have filed another nineteen cases in this district involving more than thrice that number of defendants.[1] One media outlet reports that more than 220,000 individuals have been sued since mid-2010 in mass BitTorrent lawsuits, many of them based upon alleged downloading of pornographic works.[2]

This Order addresses (1) applications by plaintiffs in three of these actions for immediate discovery, consisting of Rule 45 subpoenas directed at non-party Internet Service Providers ("ISPs") to obtain identifying information about subscribers to the named IP addresses and (2) motions to quash similar subpoenas by several putative John Doe defendants in the remaining action. For the reasons that follow, including evidence of abusive litigation tactics by plaintiffs, the plaintiffs' applications for service of subpoenas are granted only as to John Doe 1 in each case under terms and conditions set forth herein, and denied in all other respects. The motions to quash are granted because the work in that action is not subject of a copyright registration.

Furthermore, it is respectfully recommended to the respective district judges that (1) as to

---

[1] *See Patrick Collins, Inc. v. Does 1-7*, CV 11-1270 (JG) (RER) (80 defendants in consolidated case); *K-Beech, Inc. v. Does 1-29*, CV 11-3331 (JFB) (ETB); *K-Beech, Inc. v. Does 1-37*, CV 11-3741 (LDW) (AKT); *K-Beech, Inc. v. Does 1-52*, CV 11-3994 (JFB) (ETB); *Patrick Collins, Inc. & K-Beech, Inc. v. Doe*, CV 11-4094 (JFB) (GRB); *Malibu Media, LLC v. Does 1-10*, CV 12-1146 (JS) (ETB); *Malibu Media, LLC v. Does 1-20*, CV 12-1148 (ADS) (AKT); *Malibu Media, LLC v. Does 1-30*, CV 12-1149 (LDW) (AKT); *Patrick Collins, Inc. v. Does 1-11*, CV 12-1153 (JFB) (ARL); *Malibu Media, LLC v. Does 1-13*, CV 12-1156 (JFB) (ETB).

[2] *See* http://www.usnews.com/news/articles/2012/02/02/porn-companies-file-mass-piracy-lawsuits-are-you-at-risk.

three of the actions, the matters be dismissed without prejudice as to all defendants other than John Doe 1; (2) that the fourth action be dismissed without prejudice; and (3) that these plaintiffs and their counsel be directed that all future actions be filed only against a single defendant.

BACKGROUND

1. Allegations in the Complaints

The four complaints that are subject to this Order are nearly identical, though each involves a different pornographic film, to wit: *Gang Bang Virgins, Veronica Wet Orgasm, Maryjane Young Love* and *Gangbanged*. *See K-Beech, Inc. v. Does 1-37*, CV 11-3995 (DRH)(GRB) (hereinafter "*K-Beech*"); *Malibu Media LLC v. Does 1-26*, CV 12-1147(JS)(GRB) (hereinafter "*Malibu 26*"); *Malibu Media LLC v. Does 1-11*, CV 12-1150 (LDW)(GRB) (hereinafter "*Malibu 11*"); and *Patrick Collins, Inc. v. Does 1-9*, CV 12-1154 (ADS)(GRB) (hereinafter "*Patrick Collins*"). In three of the cases, plaintiff claims to be the owner of a copyright registered for the work in question. *See, e.g., Malibu 26,* Complaint at ¶¶11-13, Docket Entry ("DE") [1]. In *K-Beech,* plaintiff claims only that an application for copyright has been submitted as to its work *Gang Bang Virgins*. *K-Beech,* Am. Compl. at ¶¶11-12, DE [18]. Each defendant is identified only by an IP address purportedly corresponding to a physical address in this district, defined in the complaint as "a number that is assigned by an ISP to devices, such as computers, that are connected to the Internet." *Malibu 26,* Compl. at ¶8. The Complaints further allege that "[t]he ISP to which each Defendant subscribes can correlate the Defendant's IP address to the Defendant's true identity." *Id.* at ¶9.

The complaints describe, in some detail, a peer-to-peer filing sharing protocol known as BitTorrent which is a means by which devices connected to the Internet can share large computer files (such as digital copies of movies) while minimizing the strain on computer networks. *See,*

e.g., Malibu 26, Compl. at ¶¶14-15. BitTorrent works by breaking files into many smaller files "to reduce the load on the source computer, rather than downloading a file from a single source computer (one computer directly connected to another), [and] allows users to join a 'swarm' of host computers to download and upload from each other simultaneously (one computer connected to numerous computers)." *Id.* at ¶15. BitTorrent also uses a "tracker" computer that tracks the pieces of the files as those pieces are shared among various computers. This tracking feature the plaintiffs to identify the IP addresses from which the films were downloaded, the subscribers to which have become the defendants in these actions. *Id.* ¶¶24-26.

2. Plaintiffs' Motions for Early Discovery

Plaintiffs in *Malibu 26, Malibu 11, and Patrick Collins* have filed motions for leave to file non-party subpoenas prior to a Rule 26(f) conference, seeking to serve subpoenas upon the ISPs to identify the subscribers to the subject IP addresses. Specifically, these subpoenas seek the "true name, address, telephone number, e-mail address and Media Access Control ("MAC") address of the Defendant to whom the ISP issued an IP address." *See, e.g., Malibu 26,* Proposed Order, DE [3-2].

3. Motions to Quash

By order dated September 16, 2011, the Honorable A. Kathleen Tomlinson granted a nearly identical motion for early discovery in *K-Beech.* *See K-Beech,* Order of 9/16/11, DE [6]. However, to protect the rights of all parties, Magistrate Judge Tomlinson established a procedure by which both the ISPs and the John Does were afforded an opportunity to move to quash before the information was provided to K-Beech. The procedure Magistrate Tomlinson implemented elicited information that not only permits reasoned review of the motions to quash, but also provides insight into the pending motions for early discovery.

A total of six putative John Doe defendants moved to quash, *see K-Beech,* Motions, DE [7], [13], [14], [16], [17], & [34], while a seventh had counsel appear without filing a motion. Several motions include fact based arguments which are highly individual to each moving party, as well as legal arguments. One argument common to all of these motions arises from the fact that, according to the allegations, K-Beech does not have a registered copyright to *Gang Bang Virgins,* but premises its action on a copyright application. K-Beech has amended its complaint to include trademark allegations, but, notably, has not alleged the receipt of a copyright registration. As detailed below, the registration argument is a sufficient basis to grant the motions to quash, though not the sole basis.

4. Additional Facts

a. Factual Defenses Raised by the Moving John Doe Defendants

The factual defenses presented are vastly different and highly individualized. One movant – John Doe #16 – has stated that he was at work at the time of the alleged download. John Doe #2 states under oath that he closed the subject Earthlink account, which had been compromised by a hacker, before the alleged download. *K-Beech,* Decl. of John Doe #2, ¶5, DE [34-1]. John Doe #29's counsel represents that his client is an octogenarian with neither the wherewithal nor the interest in using BitTorrent to download *Gang Bang Virgins*. DE [13]. John Doe #10 represents that downloading a copy of this film is contrary to her "religious, moral, ethical and personal views." Mtn ¶5, DE [7]. Equally important, she notes that her wireless router was not secured and she lives near a municipal parking lot, thus providing access to countless neighbors and passersby.[3] *Id.* at ¶4

[3] While Plaintiffs claim that they can amend their complaints to allege negligence against the owner of a WiFi router who failed to password-protect the device which was then used by an intruder to infringe its copyright, *see* K-Beech

b. The Use of IP Address to Identify the Alleged Infringers

The complaints assert that the defendants – identified only by IP address – were the individuals who downloaded the subject "work" and participated in the BitTorrent swarm. However, the assumption that the person who pays for Internet access at a given location is the same individual who allegedly downloaded a single sexually explicit film is tenuous, and one that has grown more so over time. An IP address provides only the location at which one of any number of computer devices may be deployed, much like a telephone number can be used for any number of telephones. As one introductory guide states:

> If you only connect one computer to the Internet, that computer can use the address from your ISP. Many homes today, though, use routers to share a single Internet connection between multiple computers. Wireless routers have become especially popular in recent years, avoiding the need to run network cables between rooms. If you use a router to share an Internet connection, the router gets the IP address issued directly from the ISP. Then, it creates and manages a subnet for all the computers connected to that router.[4]

Thus, it is no more likely that the subscriber to an IP address carried out a particular computer function – here the purported illegal downloading of a single pornographic film – than to say an individual who pays the telephone bill made a specific telephone call.

Indeed, due to the increasingly popularity of wireless routers, it much less likely. While a decade ago, home wireless networks were nearly non-existent, 61% of US homes now have wireless access.[5] Several of the ISPs at issue in this case provide a complimentary wireless router as part of Internet service. As a result, a single IP address usually supports multiple computer

---

Mem. in Opp. at 24, DE [10], this assertion flies in the face of common sense.

4 *See* "What is an IP address?" available at http://computer.howstuffworks.com/internet/basics/question5492.htm.

5 Lardinois, F,. "Study: 61% of US Households Now Have WiFi," available at http://techcrunch.com, 4/5/12.

devices – which unlike traditional telephones can be operated simultaneously by different individuals. *See U.S. v. Latham*, 2007 WL 4563459, at *4 (D.Nev. Dec. 18, 2007). Different family members, or even visitors, could have performed the alleged downloads. Unless the wireless router has been appropriately secured (and in some cases, even if it has been secured), neighbors or passersby could access the Internet using the IP address assigned to a particular subscriber and download the plaintiff's film. As one court noted:

> In order to allow multiple computers to access the internet under the same IP address, the cable modem may be connected to a router, or may itself function as a router, which serves as a gateway through which multiple computers could access the internet at the same time under the same IP address. The router could be a wireless device in which case, computers located within 300 feet of the wireless router signal could access the internet through the router and modem under the same IP address. The wireless router signal strength could be increased beyond 600 feet if additional devices are added. The only way to prevent sharing of the wireless router is to encrypt the signal and even then an individual can bypass this security using publicly available software.

Id. at *4. Some of these IP addresses could belong to businesses or entities which provide access to its employees, customers and sometimes (such as is common in libraries or coffee shops) members of the public.

These developments cast doubt on plaintiffs' assertions that "[t]he ISP to which each Defendant subscribes can correlate the Defendant's IP address to the Defendant's true identity." *see, e.g., Malibu 26,* Compl. at ¶9, or that the subscribers to the IP addresses listed were actually the individuals who carried out the complained of acts. As one judge observed:

> The Court is concerned about the possibility that many of the names and addresses produced in response to Plaintiff's discovery request will not in fact be those of the individuals who downloaded "My Little Panties # 2." The risk is not purely speculative; **Plaintiff's counsel estimated that 30% of the names turned over by ISPs are not those of individuals who actually downloaded or shared**

> **copyrighted material.** Counsel stated that the true offender is often the "teenaged son ... or the boyfriend if it's a lady." Alternatively, the perpetrator might turn out to be a neighbor in an apartment building that uses shared IP addresses or a dormitory that uses shared wireless networks. This risk of false positives gives rise to the potential for coercing unjust settlements from innocent defendants such as individuals who want to avoid the embarrassment of having their names publicly associated with allegations of illegally downloading "My Little Panties # 2."

Digital Sin, Inc. v. Does 1-176, -- F.R.D. --, 2012 WL 263491, at *3 (S.D.N.Y. Jan. 30, 2012) (citations omitted and emphasis added). Another court noted:

> the ISP subscriber to whom a certain IP address was assigned may not be the same person who used the Internet connection for illicit purposes . . . By defining Doe Defendants as ISP subscribers who were assigned certain IP addresses, instead of the actual Internet users who allegedly engaged in infringing activity, Plaintiff's sought-after discovery has the potential to draw numerous innocent internet users into the litigation, placing a burden upon them that weighs against allowing the discovery as designed.

SBO Pictures, Inc. v. Does 1-3036, 2011 WL 6002620, at *3 (N.D.Cal. Nov. 30, 2011) (citations omitted).

In sum, although the complaints state that IP addresses are assigned to "devices" and thus by discovering the individual associated with that IP address will reveal "defendants' true identity," this is unlikely to be the case. Most, if not all, of the IP addresses will actually reflect a wireless router or other networking device, meaning that while the ISPs will provide the name of its subscriber, the alleged infringer could be the subscriber, a member of his or her family, an employee, invitee, neighbor or interloper.

c. Indicia of Unfair Litigation Tactics

One moving defendant has provided concrete evidence of improper litigation tactics employed by K-Beech. In a sworn declaration, John Doe #16 states the following:

> Upon receipt of the Complaint, I reached out to Plaintiff and spoke to a self-described "Negotiator" in an effort to see if I could prove to them (without the need for publicly tying my name to the Complaint) that I had nothing to do with the alleged copyright infringements. **The Negotiator was offered unfettered access to my computer, my employment records, and any other discovery they may need to show that I was not the culpable party.** Instead, the Negotiator refused and was only willing to settle the Complaint for thousands of dollars. While the Negotiator said on October 24, 2011 that he would check to see if he could come down from the thousands of dollar settlement amount, the Negotiator has not responded to two voice mails that were left on October 25, 2011. Notably, the Negotiator justified the settlement amount because, in part, I would incur legal fees in hiring an attorney.

K-Beech, Decl. of John Doe #16, at 11-12 , DE [16] (emphasis added). Significantly, since plaintiff has not yet been provided with the identities of the moving John Does, this record exists only because John Doe #16 proactively contacted counsel for K-Beech (who is also representing Patrick Collins, Inc. in another matter), rather than await a determination by the Court. John Doe #16's experience directly mirrors that of defendants in a separate action by plaintiff K-Beech regarding *Gang Bang Virgins*, as well as another action filed by Patrick Collins, Inc. relating to a film entitled *Cuties*. *See K-Beech, Inc. v. Does 1-85*, 2011 U.S. Dist. LEXIS 124581, at *6 (E.D.Va. Oct. 5, 2011) ("Some defendants have indicated that the plaintiff has contacted them directly with harassing telephone calls, demanding $2,900 in compensation to end the litigation") and *Patrick Collins, Inc. v. Does 1-58,* 2011 U.S. Dist. LEXIS 120235, at *6 (E.D.Va. Oct. 5, 2011) (same); *cf. Raw Films, Ltd. v. Does 1-32,* 2011 WL 6182025, at *2 (E.D.Va. Oct. 5, 2011)(same).[6]

Remarkably, plaintiff's opposition to John Doe #16's motion, encompassing 62 pages of

[6] In these cases, counsel for K-Beech and Patrick Collins, Inc. was directed to show cause why Rule 11 sanctions should not be imposed for this conduct, but ultimately sanctions were not imposed.

material,[7] does not provide any evidentiary response to these sworn assertions of improper conduct. Rather, counsel attempts to dismiss this evidence as "mere denials", and unabashedly argues that "[d]efendant's] assertion that the negotiations between him and Plaintiff have ended further supports the need for litigation." Pl's. Mem. In Opp. at 24, DE [22]. Moreover, K-Beech has filed "Notices of Settlement and Voluntary Dismissal" as to three of the John Does in this action. *See* DE [30], [31] and [38]. "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." *Raw Films,* 2011 WL 6182025, at *2.

In a similar case by plaintiff Patrick Collins filed in this district, after being granted discovery of the IP subscribers, counsel for that entity described in motion papers the intended approach to the John Doe defendants:

> Plaintiff requested and was granted additional time within which to effectuate service upon the Doe Defendants to accommodate Plaintiff's need for obtaining their identifying information, as well as its further settlement and litigation strategy. The latter involves Plaintiff contacting Doe Defendants once their identities are known and attempting to reach a settlement with them. In cases where a settlement cannot be reached, Plaintiff would then consider the feasibility of filing suit, and proceed with service upon those Doe Defendants against whom it chooses to proceed.

[7] Plaintiff K-Beech's rambling motion papers often lapse into the farcical. In its papers, counsel for K-Beech equate its difficulties with alleged piracy of its adult films with those faced by the producers of the Harry Potter books, Beatles songs and Microsoft software, and compare its efforts to collect from alleged infringers of its rights to the efforts of the FBI to combat child pornography. Mem. in Opp. at 4, 10, DE [22]. In an ironic turn, the purveyors of such works as *Gang Bang Virgins*, explain how its efforts in this matter will help empower parents to prevent minors from watching "movies that are not age appropriate" by ensuring that viewers must pay for plaintiffs products, and thereby effectively notify parents of such activity because "many parents would surely notice if they showed up on billing statements." *Id.* at 7-8. It is difficult to accord the plaintiff, which features "Teen" pornography on its website, the moral high-ground in this regard.

Patrick Collins, Inc. v. Does 1-7, CV 11-1270 (JG)(RER), Mtn, DE [22], at ¶ 6. On a cold record, this overview could be viewed as a reasoned approach. However, when viewed against undisputed experience of John Doe #16, described above, and findings by other courts, this suggests an approach that is highly inappropriate.

DISCUSSION

The Legal Standard

Federal Rule of Civil Procedure 26(d)(1) forbids a party from seeking discovery "from any source before the parties have conferred as required by Rule 26(f) except as "authorized ... by court order." Fed. R. Civ. P. 26(d) (1). This is generally viewed as requiring a showing of good cause. *See, e.g., Ayyash v. Bank Al–Madina,* 233 F.R.D. 325, 326 (S.D.N.Y. 2005). Plaintiffs rely principally upon the five factor *Sony Music* test, adopted by the Second Circuit, which requires the Court to weigh:

> (1) [the] concrete[ness of the plaintiff's] showing of a prima facie claim of actionable harm, ... (2) [the] specificity of the discovery request, ... (3) the absence of alternative means to obtain the subpoenaed information, ... (4) [the] need for the subpoenaed information to advance the claim, ... and (5) the [objecting] party's expectation of privacy.

Arista Records, LLC v. Doe 3, 604 F.3d 110, 119 (2d Cir. 2010) (*citing Sony Music Entm't Inc. v. Does 1–40,* 326 F. Supp. 2d 556, 564–65 (S.D.N.Y. 2004)). This test, articulated in the context of evaluating a motion to quash, frames the inquiry in evaluating defendants' motions in *K-Beech.* Additionally, plaintiffs correctly note that the test is also instructive in evaluating the motions for early discovery.

Element 1: Prima Facie Claim of Actionable Harm

Plaintiffs Malibu and Patrick Collins have set forth *prima facie* claims of actionable harm

by alleging ownership of registered, copyrighted works that have been infringed.[8]

The situation with K-Beech is far different. K-Beech does not allege that it has a copyright registration; rather, it bases its complaint on a copyright application. In another case in this district, *K-Beech v. Does 1-29*, CV 11-3331, Magistrate Judge Boyle denied K-Beech the precise relief sought in the instant application based on a failure to allege that its copyright in the work in that case – *Virgins 4* – had been registered. Judge Boyle found:

> Section 411(a) of the Copyright Act "requires copyright holders to register their works before suing for copyright infringement." *Reed Elsevier, Inc. v. Muchnick*, — U.S. —, 130 S. Ct. 1237, 1241, 176 L. Ed. 2d 18 (2010) (citing 17 U.S.C.A. § 411(a)). While failure to register a work does not deprive a federal court of jurisdiction over an action for infringement, valid registration is an element of an infringement claim. Although the Second Circuit has not addressed this specific question, courts in both the Eastern District of New York and the Southern District of New York have held that submission of an application for copyright registration does not satisfy the registration precondition of § 411(a).

Order of 9/19/11 at 2-3 (additional quotations and citations omitted), DE [10]. Judge Boyle denied the requested discovery, and K-Beech voluntarily dismissed the case. *See* DE [12]. I agree with Judge Boyle and find that K-Beech has not met its burden on this factor.

K-Beech attempted to remedy this deficiency by adding conclusory trademark claims to its amended complaint. The complaint fails to explain in what ways the illegal downloading and uploading alleged could possibly cause confusion among consumers, or "hamper efforts by

[8] For the purposes of this analysis, it is assumed that plaintiffs' works are entitled to copyright protection, though that may be an open question. *See Liberty Media Holdings, LLC v. Swarm Sharing Hash File*, 821 F. Supp. 2d 444, 447 n.2 (D.Mass. 2011) (it is "unsettled in many circuits, whether pornography is in fact entitled to protection against copyright infringement").

Plaintiff to protect its reputation" with "the purchasing public in New York."[9] Am. Compl. ¶¶64-67, DE [18]. K-Beech's citation to *dicta* in the Supreme Court's decision in *Dastar* is unavailing, as that case's holding undercuts plaintiff's attempt to extend trademark protection to these facts. *Dastar Corp. v. Twentieth Century Fox Film Corp.*, 539 U.S. 23, 34 (2003) ("in construing the Lanham Act. we have been careful to caution against misuse or over-extension of trademark and related protections into areas traditionally occupied by copyright" (citation omitted)). Even viewed in the most favorable light, the trademark allegations fail to state a claim.

Elements 2: The Specificity of the Discovery Requests

With respect to the specificity of discovery requests, the *Sony Music* court explained that this factor requires that "Plaintiffs' discovery request is also sufficiently specific to establish a reasonable likelihood that the discovery request would lead to identifying information that would make possible service upon particular defendants who could be sued in federal court." *Sony Music*, 326 F. Supp. 2d at 566. While the discovery propounded by plaintiffs is specific, for the reasons discussed above, it does not establish a reasonable likelihood it will lead to the identity of defendants who could be sued. *See Pacific Century Int'l Ltd. v. Does*, 2011 WL 5117424, at *2 (N.D.Cal. Oct. 27, 2011) ("Plaintiff must go beyond the 'limited discovery' that it earlier asserted would lead to Defendants' identities . . . [p]resumably, every desktop, laptop, smartphone, and tablet in the subscriber's residence, and perhaps any residence of any neighbor, houseguest or other

[9] As K-Beech put its reputation into issue, it is worth noting that the owner of K-Beech Inc. (and the apparent inspiration for the K-Beech mark) is Kevin Beechum. *See* "Porn studios raided to ensure adult-only casts," 1/12/07, *LA Times* at 1. It appears that this is the same Kevin Beechum who testified in federal prosecutions about his experience vandalizing retail adult video stores to help extort protection payments from their owners. *See U.S. v. Feinberg*, 89 F.3d 333, 335 (7th Cir. 1996); *U.S. v. Sturman*, 49 F.3d 1275, 1278 (7th Cir. 1995). In those cases, Beechum described how he hired associates to use hammers and baseball bats to inflict $10,000 in damage on a Phoenix adult shop, and negotiated over a "few more jobs" in Cleveland. Other evidence established that, following Beechum's introduction, these same associates, on behalf of the extortionists, planned to plant remote control bombs at eight stores in Chicago in furtherance of the scheme, but that plan failed when, after successfully attacking one store, a bomb accidentally went off, killing one of the coconspirators.

sharing his internet access, would be fair game. Beyond such an inspection, [the plaintiff] might require still more discovery, including interrogatories, document requests and even depositions." (citations omitted; alterations in original)).

In this regard, the instant matter is factually distinguishable from the *Arista Records* decision. In that case, the sought after discovery involved an Internet service provider located at a university. Based on that setting, and at that time, it was almost certain that the end user at an IP address was a particular individual, rather than a wireless network. The instant case involves broadband Internet service in a largely residential suburban area at a time when wireless is widely available. Furthermore, it is alleged that each John Doe in the instant case downloaded only a single pornographic film. By contrast, in *Arista Records*, the plaintiff alleged that a file sharing folder located at the IP address in question contained 236 audio files, containing at least a half-dozen copyrighted songs owned by the plaintiff. *Arista Records,* 604 F.3d at 122. In fact, in that case, plaintiffs' investigator was able to "download[] music files from the user's computer," which is not the case here. *Arista Records LLC v. Does 1-16,* 2009 WL 414060, at *1 (N.D.N.Y. Feb. 18, 2009) *aff'd* 604 F.3d 110 (2d Cir. 2010). Clearly, the level of activity in *Arista Records* made it far more likely that the subscriber to the IP address would have conducted or at least been aware of the illegal downloading. In sum, it is not clear that plaintiffs have satisfied this factor.

Element 3: The Absence of Alternative Means

As one court observed, "[b]ecause the transactions in question occurred online, the defendants have been elusive and the IP addresses and ISP are the only available identifying information. Without the requested discovery, there are no other measures Plaintiff can take to identify the personal information for the Doe defendants." *Raw Films, Ltd. v. Does 1-11,* 2012 WL 684763, at *2 (S.D. Cal. Mar. 2, 2012). Plaintiffs retained a company that provides forensic

investigation services including the identification of IP addresses using BitTorrent protocol. *See* Fieser Decl. ¶¶5-6. DE [3-3]. Since plaintiffs have only been able to identify IP addresses used for potential infringement, they have established to the satisfaction of the Court that there are not alternative means available to identify the alleged infringers.

Element 4: The Need for Subpoenaed Information to Advance the Claim

Plaintiffs clearly need identification of the putative John Does in order to serve process on them and prosecute their claims. However, not all the information sought is required to advance the claim. For example, in addition to names and addresses, plaintiffs seek both the home telephone numbers and email addresses of the putative John Does, *see Malibu 26,* Proposed Order DE [3-2], information which is clearly not required to proceed with this action. In particular, obtaining the home telephone numbers seems calculated to further plaintiffs' settlement strategies, discussed above, rather than advancing their claims by allowing them to effect service.

Element 5: Defendants' Expectation of Privacy

In *Arista Records*, the John Doe defendant, conceding that he had engaged in the alleged improper downloading, sought to quash the subpoena on First Amendment grounds. While recognizing the protected nature of anonymous speech, the Court rejected the challenge, concluding that the "First Amendment does not . . . provide a license for copyright infringement." *Arista Records,* 604 F.3d at 118. In examining this factor, the *Sony Music* court noted "defendants have little expectation of privacy in downloading and distributing copyrighted songs without permission." *Sony Music,* 326 F. Supp. 2d at 566-67. Here it is uncertain – indeed, it may be unlikely – that the subscribers sought to be identified downloaded the plaintiffs' copyrighted works. *Cf. Pacific Century,* 2011 WL 5117424, at *2 (denying discovery to protect "innocent internet users"). Thus, this Court cannot conclude with any reasonable certainty that

plaintiffs have overcome the expectation of privacy by putative defendants.

Abusive Litigation Tactics Employed by the Plaintiffs

The most persuasive argument against permitting plaintiffs to proceed with early discovery arises from the clear indicia, both in this case and in related matters, that plaintiffs have employed abusive litigations tactics to extract settlements from John Doe defendants. Indeed, this may be the principal purpose of these actions, and these tactics distinguish these plaintiffs from other copyright holders with whom they repeatedly compare themselves. *See, e.g., K-Beech*, Pl. Mem. in Opp. at 3, DE [22] (arguing that this decision "will affect the rights of intellectual property holders across all segments of society"). While not formally one of the *Sony Music* factors, these facts could be viewed as a heightened basis for protecting the privacy of the putative defendants, or simply grounds to deny the requested discovery on the basis of fundamental fairness.

In an effort to defend its litigation approach, K-Beech argues that "Fed.R.Civ.P. 1 requires that Courts construe the rules to secure the inexpensive determination of every action." Pl. Mem. in Opp. at 11, DE [22]. This Court takes the mandate of Rule 1 quite seriously, and vigorously encourages efforts by litigants to reduce litigation costs through settlement. *See In re Tobacco Litig.*, 192 F.R.D. 90, 95 (E.D.N.Y. 2000) (describing court's "duty to take affirmative action assisting the parties in all possible settlement options"). However, in its argument, plaintiff neglects to observe that Rule 1 requires that disputes should be resolved in a manner that is "**just**, speedy and inexpensive." Fed. R. Civ. P. 1 (emphasis added). In this case, John Doe #16 offered the plaintiff "unfettered access" to his computer and employment records demonstrating that he was not at home at the time of the downloading, yet still finds himself pressured to settle for thousands of dollars. It would be difficult to characterize such a resolution as "just" even if speedy and inexpensive (for the plaintiff). *Cf. On The Cheap, LLC v. Does 1-5011*, -- F.R.D. --,

2011 WL 4018258, at *4 (N.D.Cal. Sept. 6, 2011) ("plaintiff's desire to enforce its copyright in what it asserts is a cost-effective manner does not justify perverting the joinder rules to first create . . . management and logistical problems . . . and then offer to settle with Doe defendants so that they can avoid digging themselves out of the morass plaintiff is creating").

Our federal court system provides litigants with some of the finest tools available to assist in resolving disputes; the courts should not, however, permit those tools to be used as a bludgeon. As one court advised Patrick Collins Inc. in an earlier case, "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." *Patrick Collins, Inc. v. Does 1–3757*, 2011 U.S. Dist. LEXIS 128029, at *6–7 (N.D.Cal. Nov. 4, 2011).

Given the unopposed, sworn account by John Doe #16, which dovetails with the experience of defendants in other actions brought by K-Beech and Patrick Collins, I find counsel for K-Beech has already engaged in improper litigation tactics in this matter, and find it highly probable that Patrick Collins Inc. and Malibu will likely engage in similar tactics if permitted to proceed with these mass litigations. Such conduct cannot be condoned by this Court. This is a persuasive basis to deny the motions for early discovery, as well as an additional basis to grant the motions to quash. *See Pacific Century*, 2011 WL 5117424, at *2 (denying discovery on this basis).

It would be unrealistic to ignore the nature of plaintiffs' allegations – to wit: the theft of pornographic films – which distinguish these cases from garden variety copyright actions. Concern with being publicly charged with downloading pornographic films is, understandably, a common theme among the moving defendants. As one woman noted in *K-Beech*, "having my

name or identifying or personal information further associated with the work is embarrassing, damaging to my reputation in the community at large and in my religious community." Mtn to Quash, ¶5, DE [7]. Many courts evaluating similar cases have shared this concern. *See,e.g., Pacific Century Int'l, Ltd. v. Does 1-37,* – F. Supp. 2d –, 2012 WL 1072312, at *3 (N.D. Ill. Mar. 30, 2012) ("the subscribers, often embarrassed about the prospect of being named in a suit involving pornographic movies, settle"); *Digital Sin,* 2012 WL 263491, at *3 ("This concern, and its potential impact on social and economic relationships, could compel a defendant entirely innocent of the alleged conduct to enter an extortionate settlement") *SBO Pictures,* 2011 WL 6002620, at *3 (defendants "whether guilty of copyright infringement or not-would then have to decide whether to pay money to retain legal assistance to fight the claim that he or she illegally downloaded sexually explicit materials, or pay the money demanded. This creates great potential for a coercive and unjust 'settlement'"). This consideration is not present in infringement actions involving, for example, popular music downloads. *See Arista Records,* 604 F.3d at 122, ("Teenagers and young adults who have access to the Internet like to swap computer files containing popular music . . . The swappers . . . are ignorant or more commonly disdainful of copyright." (*quoting In re Aimster Copyright Litig.*, 334 F.3d 643, 645 (7th Cir. 2003))).

The Federal Rules direct the Court to deny discovery "to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense." Fed. R. Civ. P. 26(c)(1). This situation cries out for such relief.

Joinder is Inappropriate

In opposing the motions to quash, K-Beech relies heavily on the "swarm joinder" theory championed by plaintiffs here and elsewhere. Rule 20 governs the permissive joinder of parties and states that defendants may be joined in one action where a plaintiff states a right to relief

"arising out of the same transaction, occurrence, or series of transactions or occurrences" and "any question of law or fact common to all defendants will arise in the action." Fed. R. Civ. P. 20 (a) (2) (A) & (B). The argument is that every user who participates in the "swarm" is acting in concert to violate plaintiffs' copyrights.

Highly questionable factual assumptions underlie plaintiffs' contention that these cases satisfy the Rule 20 requisites for joinder. By way of example, Plaintiffs assert that the John Does were "acting in concert with each other," "working together", and "directly interacted and communicated with other members of that swarm." *See, e.g., Malibu 26,* Compl. ¶¶ 10, 33, 34. Much of the BitTorrent protocol operates invisibly to the user – after downloading a file, subsequent uploading takes place automatically if the user fails to close the program. Exhibit D to the complaints, which allegedly documents the "interactions" between defendants, is a page of machine instructions which clearly demonstrate that the user plays no role in these interactions. Indeed, "[t]he bare fact that Doe clicked on a command to participate in the BitTorrent Protocol does not mean that they were part of the downloading by unknown hundreds or thousands of individuals across the country or across the world." *Hard Drive Prods., Inc. v. Does 1-188,* 809 F. Supp. 2d 1150, 1163 (N.D. Cal. 2011).

Moreover, the dates of downloading provided in the complaints – which are often weeks or months apart -- further undermine the allegation that all of the John Does were part of a single swarm. Thus, *even assuming that the John Does are the actual infringers*, the assertion that defendants were acting in concert rests upon a thin reed. *See generally Raw Films, Ltd. v. Does 1-32,* 2011 WL 6840590, at *2 (N.D.Ga. Dec. 29, 2011) (stating that the "differing dates and times of each Defendant's alleged sharing do not allow for an inference that the Defendants were acting in concert"); *Raw Films, Ltd. v. Does 1-32,* 2011 WL 6182025 at *2 (E.D.Va. 2011) (conduct over

a three month time span was "insufficient to meet the standards of joinder set forth in Rule 20"). I find that plaintiffs have not satisfied the requirement of establishing that defendants participated in the same "transaction" or "occurrence" within the meaning of Rule 20.

Alternatively, because joinder is permissive, this Court retains the discretion to sever under Rules 20(b), 21, and 42 (b). *See Third Degree Films v. Does 1-131,* -- F. Supp. 2d --, 2012 WL 692993, at *3 (D. Ariz. Mar. 1, 2012). In determining whether to exercise that discretion, the court should "examine whether permissive joinder would comport with the principles of fundamental fairness or would result in prejudice to either side." *On the Cheap,* 2011 WL 4018258, at *2 (quoting *Coleman v. Quaker Oats Co.,* 232 F.3d 1271, 1296 (9th Cir. 2000)). "Courts may also consider factors such as the motives of the party seeking joinder and whether joinder would confuse and complicate the issues for the parties involved." *SBO Pictures,* 2011 WL 6002620, at *3.

Plaintiffs identify two common questions of fact in these actions: the plaintiffs' ownership of copyrights, and the workings of BitTorrent. By contrast, the half-dozen moving defendants, even at this preliminary stage, have raised a panoply of individual defenses, including age, religious convictions, and technological savvy; misidentification of ISP accounts; the kinds of WiFi equipment and security software utilized; and the location of defendant's router. The individualized determinations required far outweigh the common questions in terms of discovery, evidence, and effort required. Thus, swarm joinder complicates these actions, resulting in waste of judicial resources.

Plaintiffs tout the fact that "joinder in BitTorrent copyright infringement cases has been thoroughly analyzed in forty reported opinions and has been permitted in district courts across the country." *K-Beech,* Mem. in Opp. at 1, DE [25]. However, due to plaintiffs' litigation

strategy, which includes avoiding review on the merits except at a preliminary, *ex parte* stage, these determinations were made without any factual record by judges unaware of the highly individualized, fact specific defenses raised on the motions to quash, or evidence of strong-arm tactics, both of which strongly militate against allowing joinder in these mass actions.

On this issue, one court has observed:

> In addition to the Rule 20(a)(2) criteria, the court has a parallel duty to ensure that permissive joinder "would comport with the principles of fundamental fairness or would [not] result in prejudice to either side. The court also has discretion to sever an action when joinder would confuse and complicate the issues for all parties involved. It is likely that Defendants would assert different factual and legal defenses, and would identify different witnesses. Case management and trial . . . would be inefficient, chaotic, and expensive. Joining Defendants to resolve what at least superficially appears to be a relatively straightforward case would in fact transform it into a cumbersome procedural albatross. These difficulties would place tremendous burden on Defendants as well. To provide two illustrative examples, each Defendant would have the right to be present at every other Defendant's depositions—a thoroughly unmanageable and expensive ordeal. Similarly, *pro se* Defendants, who most likely would not e-file, would be required to serve every other Defendant with a copy of their pleadings and other submissions throughout the pendency of the action at substantial cost. The court cannot permit a case to proceed in this manner.

Pacific Century, 2011 WL 5117424, at *3 (quotations and citations omitted). As such, I find that principles of fundamental fairness and judicial economy dictate that permissive joinder not be allowed in these cases.

By Pursuing Mass Actions, Plaintiffs Improperly Avoid Payment of Filing Fees

The payment of court filing fees is mandated by statute. Specifically, the "district court shall require the parties instituting any civil action, suit or proceeding in such court, whether by original process, removal or otherwise, to pay a filing fee of $350." 28 U.S.C. §1914(a). Of that

amount, "$190 shall be deposited into a special fund of the Treasury to be available to offset funds appropriated for the operation and maintenance of the courts of the United States." 28 U.S.C. §1931(1).

In multidistrict cases considering severance of cases, courts have noted that the filing fee has:

> two salutory purposes. First, it is a revenue raising measure. . . Second, §1914(a) acts as a threshold barrier, albeit a modest one, against the filing of frivolous or otherwise meritless lawsuits. Had each plaintiff initially instituted a separate lawsuit as should have occurred here, a fee would have been collected for each one. . . . Thus, the federal fisc and more particularly the federal courts are being wrongfully deprived of their due. By misjoining claims, a lawyer or party need not balance the payment of the filing fee against the merits of the claim or claims.

In re Diet Drugs, 325 F. Supp. 2d 540, 541-42 (E.D. Pa. 2004); *see also In re Seroquel Prods. Liability Litig.,* 2007 WL 737589, at *2-3 (M.D. Fla. Mar. 7, 2007) (denying reduction of filing fees, noting the burden on the court and the "gatekeeping feature of a filing fee").

Several courts in similar cases involving BitTorrent protocol have also recognized the effect of a countenancing a single filing fee. One court described the "common arc of the plaintiffs' litigating tactics" in these cases:

> ...these mass copyright infringement cases have emerged as a strong tool for leveraging settlements–a tool whose efficacy is largely derived from the plaintiffs' success in avoiding the filing fees for multiple suits and gaining early access en masse to the identities of alleged infringers.

Pacific Century, 2012 WL 1072312, at *3. Thus, the plaintiffs file a single case, and pay one filing fee, to limit their expenses as against the amount of settlements they are able to negotiate. Postponing a determination on joinder in these cases "results in lost revenue of perhaps millions of dollars (from lost filing fees) and only encourages plaintiffs in copyright actions to join (or

misjoin) as many doe defendants as possible." *K-Beech, Inc. v. John Does 1-41,* 2012 WL 773683, at *5 (S.D. Tex. 2012).

In the four cases before this Court, plaintiffs have improperly avoided more than $25,000 in filing fees by employing its swarm joinder theory. Considering all the cases filed by just these three plaintiffs in this district, more than $100,000 in filing fees have been evaded. If the reported estimates that hundreds of thousands of such defendants have been sued nationwide, plaintiffs in similar actions may be evading millions of dollars in filing fees annually. Nationwide, these plaintiffs have availed themselves of the resources of the court system on a scale rarely seen. It seems improper that they should profit without paying statutorily required fees.

CONCLUSION

Because K-Beech has failed to allege a valid cause of action, and for all the other reasons set forth herein, the motions to quash in *K-Beech,* CV 11-3995, DE [7], [13], [14], [16], [17], [34], are hereby GRANTED.

For all of the reasons set forth herein, the Court is not inclined to grant the broad early discovery sought by Malibu and Patrick Collins. At the same time, these plaintiffs are allegedly the owners of copyrighted works who should not be left without any remedy. Given the record in this case, however, this must be done in a fashion that will ensure that the rights of all parties are adequately protected. Thus, the Court is prepared to grant these plaintiffs limited early discovery, to wit: the names and addresses (**not** email addresses or phone numbers) of **only** the subscribers designated as John Doe 1 in *Malibu 26, Malibu 11, and Patrick Collins*. Following service of subpoenas, under the terms and conditions set forth below, the identifying information will be provided to plaintiffs at a status conference, with each John Doe 1 present, giving them an opportunity to be heard, to obtain counsel and, if appropriate, request appointment of counsel from

this Court's *pro bono* panel.

Plaintiffs' motions for leave to serve third-party subpoenas prior to a Rule 26(f) conference, *Malibu 26,* CV 12-1147, DE [3], *Malibu 11,* CV 12-1150, DE [3], and *Patrick Collins,* CV 12-1154, DE [3], are GRANTED ONLY to the following extent:

(1) Plaintiffs in *Malibu 26. Malibu 11 and Patrick Collins* may serve subpoenas pursuant to Rule 45 of the Federal Rules of Civil Procedure on the ISPs to obtain the name, address, and Media Access Control address for each Defendant designated as John Doe 1 in each action to whom the ISP assigned an IP address. Under no circumstances are plaintiffs permitted to seek or obtain the telephone numbers or email addresses of these individuals, or to seek or obtain information about any potential John Doe defendant other than John Doe 1. Plaintiff's counsel is directed to attach a copy of this Order to the subpoena.

(2) Within seven days of service of each subpoena, the ISPs shall reasonably attempt to identify each John Doe 1 and provide him or her with a copy of the subpoena and this Order. If any of the ISPs are unable to determine, to a reasonable degree of technical certainty, the identity of the user of a particular IP address, it shall so notify Plaintiff's counsel.

(3) The ISPs shall have twenty-one (21) days from the service of the subpoena to move to quash or otherwise object to the subpoena. Each potential defendant shall have fourteen (14) days from receipt of the subpoena from the ISP to move to quash or otherwise object to the subpoena.

(4) Absent any motion to quash or objection, **the ISPs shall produce the information sought to the Court, not to the Plaintiff** within twenty-one (21) days after notifying

each Defendant pursuant to paragraph (2) above. Said submission shall be made *ex parte* and under seal. Said information will be provided to counsel for plaintiffs at a status conference to be scheduled by the Court.

(5) Plaintiff may only use the information disclosed pursuant to the subpoenas for the purpose of protecting and enforcing Plaintiffs' rights as set forth in the Complaint.

REPORT AND RECOMMENDATION TO THE DISTRICT JUDGES

For all of the reasons set forth herein, it is respectfully recommended as follows:

1. That the complaints in *Malibu 26, Malibu 11 and Patrick Collins* be dismissed, *sua sponte* and without prejudice, as to all defendants other than the individual designated as John Doe 1 in each action;
2. That the complaint in *K-Beech* be dismissed, *sua sponte* and without prejudice, in its entirety; and
3. That plaintiffs and their counsel in all four actions be directed that any future actions of a similar nature in this district be filed as separate actions as against each John Doe defendant, so as to avoid unfair outcomes, improper joinder and waste of judicial resources, and to ensure the proper payment of filing fees. *See, e.g., DIRECTV, Inc. v. Armellino,* 216 F.R.D. 240, 241 (E.D.N.Y. 2003) (Spatt, J.) ("plaintiff is advised that all future claims of this nature must be instituted separately against individual defendants"), (*citing CSC Holdings Inc. v. Tack*, CV 00–3555 (E.D.N.Y. June 16, 2000) (Seybert, J.)).

A copy of this Order and Report and Recommendation is being sent to counsel for the

plaintiffs by electronic filing on the date below. Any objections to the Report and Recommendation portion must be filed with the Clerk of the Court within 14 days. *See* 28 U.S.C. §636 (b)(1); Fed. R. Civ. P. 72; Fed. R. Civ. P. 6(a) and 6(d). Failure to file objections within this period waives the right to appeal the District Court's Order. *See Ferrer v. Woliver*, 2008 WL 4951035, at *2 (2d Cir. Nov. 20, 2008); *Beverly v. Walker*, 118 F.3d 900, 902 (2d Cir. 1997); *Savoie v. Merchants Bank*, 84 F.3d 52, 60 (2d Cir. 1996).

Dated: Central Islip, New York
May 1, 2012

/s/ Gary R. Brown
GARY R. BROWN
United States Magistrate Judge

EXHIBIT C

1) The date that Plaintiff's counsel served subpoenas on each ISP and the date the ISP responded.

ISP	Issued	Response
Advanced Colocation	8/5/11	
Covad Communications Co.	8/5/11	
AT&T Internet Services	8/5/11	11/15/11
Color Broadband	8/5/11	8/18/11
Sonic	8/5/11	
Charter Communications	8/5/11	11/15/11
Comcast Cable Communications	8/5/11	10/10/11
Frontier Communications of America	8/5/11	
Sprint PCS	8/5/11	
Unwired Broadband	8/5/11	8/18/11
Black Oak Computers	8/5/11	9/26/11
Wave Broadband	8/5/11	10/24/11
Clearwire US	8/5/11	
Verizon Online	8/5/11	
Surewest Broadband	8/5/11	
Cox Communications	8/5/11	11/28/11

2) The IP addresses for which Plaintiff's counsel has made a settlement offer and how that offer was communicated, e.g. by mail, phone, or email. The movants (for motions to quash) and objectors to whom Plaintiff's counsel has made a settlement offer and how that offer was communicated.

Status	IP
USMail	67.121.209.48
USMail	66.215.158.202
USMail	68.101.114.52
USMail	68.113.62.22
USMail	67.181.128.221
USMail	69.107.102.11
USMail	64.203.113.177
USMail	67.161.66.97
USMail	69.108.96.77
USMail	99.183.240.55
USMail	98.210.25.174
USMail	98.207.38.44
USMail	68.4.128.139
USMail	68.5.188.159
USMail	69.227.70.219
USMail	69.107.91.219
USMail	76.20.11.145
USMail	71.195.97.154
USMail	72.220.176.44
USMail	76.126.36.154
USMail	76.103.48.164
USMail	24.5.13.184
USMail	68.127.118.133
USMail	68.5.122.173
USMail	68.7.130.203
USMail	68.8.57.53
USMail	71.202.113.106
USMail	76.127.112.56
USMail	24.6.249.176
USMail	67.166.151.220
USMail	67.180.246.80
USMail	76.14.29.230
USMail	76.254.41.180
USMail	24.23.6.73
USMail	71.198.194.113
USMail	72.211.231.103
USMail	72.197.231.3
USMail	24.4.144.239
USMail	71.198.158.39
USMail	72.220.42.29
USMail	76.230.233.239
USMail	24.23.222.237
USMail	209.237.232.57
USMail	108.81.168.247
USMail	24.180.49.171
USMail	24.5.38.201
USMail	98.207.183.169
USMail	24.205.30.192
USMail	67.180.56.26
USMail	68.126.204.146
USMail	68.111.244.226
USMail	68.105.66.166
USMail	72.197.43.207
USMail	98.208.108.119
USMail	98.182.27.239
USMail	98.207.248.39
USMail	98.234.59.149
USMail	24.4.119.18
USMail	24.6.73.58
USMail	174.65.129.8
USMail	76.126.155.41
USMail	76.126.66.211
USMail	71.204.161.2
USMail	76.200.129.112
USMail	70.181.85.58
USMail	71.202.249.178
USMail	74.213.246.188
USMail	98.192.186.87
USMail	99.183.242.47
USMail	98.176.78.121
USMail	99.24.161.31
USMail	98.234.38.72
USMail	98.210.218.152
USMail	98.238.203.2
USMail	99.183.243.142
USMail	98.176.15.188
USMail	98.248.213.208
USMail	99.41.79.188
USMail	67.169.107.114
USMail	67.187.248.194

In cases where a motion to quash was filed.

Status	IP
USMail	71.139.12.128

USMail 71.83.208.158

3) A list of ISPs not complying with Magistrate Judge Lloyd's expedited discovery order, and for which IP addresses the ISP is not complying. Include the reason, if any, given by the ISP for not complying.

ISP	IP Addresses	Reason
Advanced Colocation	ALL	None provided
Black Oak Computers	66.160.133.102	Two Subpoenas issued, one completed, the other no response, no reason provided
Clearwire US	ALL	None provided
Covad Communications Co.	ALL	None provided
Frontier Communications of America	ALL	None provided
Sonic	ALL	None provided
Sprint PCS	ALL	None provided
Surewest Broadband	ALL	None provided
Verizon Online	ALL	None provided

4) A list of ISPs not complying with a subpoena, and for which IP addresses the ISP is not complying. Include the reason, if any, given by the ISP for not complying.

ISP	IP Addresses	Reason
Advanced Colocation	ALL	None provided
Black Oak Computers	66.160.133.102	Two Subpoenas issued, one completed, the other no response, no reason provided
Clearwire US	ALL	None provided
Covad Communications Co.	ALL	None provided
Frontier Communications of America	ALL	None provided
Sonic	ALL	None provided
Sprint PCS	ALL	None provided
Surewest Broadband	0	None provided
Verizon Online	0	None provided

5) A list of the ISPs for which there is a pending motion to quash.
AT&T, COMCAST, CHARTER & COX

6) Whether, when, and by what means Plaintiff's counsel has contacted John Doe 134, the movant in ECF No. 25.
Plaintiff's counsel has not attempted to contact the unidentified individual referred to by the Court as "John Doe 134."

7) Whether, when, and by what means Plaintiff's counsel has contacted or attempted to contact Messrs. Ferlito and Smith.
Plaintiff's counsel attempted to contact Mr Ferlito by U.S mail. Plaintiff's counsel attempted to contact Mr. Smith by U.S. mail.

8) A list of the IP addresses for which Plaintiff's counsel received subpoena returns and whether the ISP provided all the categories of information requested by the subpoena. If the ISP did not provide all categories of information, identify which categories of information were not provided.

IP Address	Missing		email	76.200.129.112	Phone, email
68.126.204.146	Phone, email	69.107.91.219	Phone, email	76.254.41.180	Phone, email
68.127.118.133	Phone, email	69.108.96.77	Phone	99.183.240.55	Phone, email
69.107.102.11	Phone,	69.227.70.219	Phone		
		71.139.12.128	Email		

99.183.242.47	Phone, email	24.5.13.184	Email	76.126.66.211	Email
		67.161.66.97	Email	98.192.186.87	Email
99.183.243.142	Phone, email	67.166.151.220	Email	98.207.248.39	Email
		67.169.107.114	Email	98.208.108.119	Email
99.24.161.31	Phone, email	67.180.56.26	Email	98.210.218.152	Email
		67.181.128.221	Email	98.210.25.174	Email
99.41.79.188	Phone	67.187.248.194	Email	98.234.128.170	Email
209.237.232.57	Phone	71.198.158.39	Email	98.234.38.72	Email
68.113.62.22	Email	71.202.113.106	Email	98.234.59.149	Email
74.213.246.188	Email	71.202.249.178	Email	98.248.213.208	Email
24.23.222.237	Email	76.103.48.164	Email	68.101.114.52	Email
24.23.6.73	Email	76.126.155.41	Email	72.197.231.3	Phone, email
24.4.144.239	Email	76.126.36.154	Email		

9) A list of the BitTorrent copyright infringement cases involving multiple joined John Doe Defendants filed Plaintiff's counsel's law firm or predecessor firm in federal court. Identify the case by name, case number, court, and filing date. For each case, indicate how many Doe Defendants were actually served.

Although our records indicate that we have filed suits against individual copyright infringement defendants, our records indicate that no defendants have been served in the below-listed cases.

Case Name	Case Number	Court	Filing date
Lightspeed Media Corporation v. Does 1-9	4:11-cv-02261	ND CA	5/6/11
MCGIP, LLC v. Does 1-9	3:11-cv-02262	ND CA	5/6/11
CP Productions, Inc. v. Does 1-300	1:10-cv-06255	ND IL	9/29/10
Future Blue, Inc. v. Does 1-300	1:10-cv-06256	ND IL	9/29/10
First Time Videos LLC v. Does 1-500	1:10-cv-06254	ND IL	9/29/11
Hard Drive Productions, Inc.v. Does 1-100	1:10-cv-05606	ND IL	9/2/10
Lightspeed Media Corporation v. Does 1-100	1:10-cv-05604	ND IL	9/2/10
Millennium TGA, Inc. v. Does 1-100	1:10-cv-05603	ND IL	9/2/10
In the Matter Of a Petittion By Ingenuity13 LLC	2:11-mc-00084	ED CA	10/28/11
Pacific Century International Ltd. v. Does 1-101	4:11-cv-02533	ND CA	5/25/11
Boy Racer Inc. v. Does 1-10	1:11-cv-00592	SD OH	8/26/11
Hard Drive Productions, Inc. v. Does 1-10	1:11-cv-02980	ND IL	5/4/11
Boy Racer Inc. v. Does 1-10	3:11-cv-00492	WD KY	8/31/11
CP Productions, Inc. v. Does 1-12	3:11-cv-02259	ND CA	5/6/11
Hard Drive Productions, Inc. v. Does 1-11	1:11-cv-23033	SD FL	8/23/11
Hard Drive Productions, Inc. v. Does 1-12	1:11-cv-00595	SD OH	8/26/11
MCGIP, LLC v. Does 1-14	1:11-cv-02887	ND IL	4/29/11
CP Productions, Inc. v. Does 1-14	1:11-cv-22204	SD FL	6/17/11
Hard Drive Productions, Inc. v. Does 1-14	1:11-cv-02981	ND IL	5/4/11
Pacific Century International LTD v. Does 1-14	1:11-cv-03118	ND IL	5/10/11
Boy Racer Inc. v. Does 1-17	1:11-cv-05416	ND IL	8/10/11
MCGIP, LLC v. Does 1-316	1:10-cv-06677	ND IL	10/15/10
Hard Drive Productions, Inv. v. Does 1-16	1:11-cv-23064	SD FL	8/25/11
Hard Drive Productions, Inc. v. Does 1-16	1:11-cv-03108	ND IL	5/10/11
VPR Internationale v. Does 1-17	4:11-cv-01494	ND CA	3/28/11
First Time Videos LLC v. Does 1-18	4:11-cv-00069	SD IN	6/14/11
MCGIP, LLC v. Does 1-17	3:11-cv-50062	ND IL	3/9/11
Boy Racer Inc. v. Does 1-17	1:11-cv-03097	ND IL	5/9/11
VPR International v. Does 1-1017	2:11-cv-02068	ND IL	3/8/11
Hard Drive Productions, Inc. v. Does 1-118	4:11-cv-01567	ND CA	3/3/11
Hard Drive Productions, Inv. v. Does 1-18	1:11-cv-23032	SD FL	8/23/11

MCGIP, LLC v. Does 1-18	3:11-cv-01495	ND CA	3/28/11
Pink Lotus Entertainment LLC v. Does 1-20	1:11-cv-03048	ND IL	5/6/11
MCGIP, LLC v. Does 1-20	1:11-cv-04486	ND IL	7/1/11
Millennium TGA, inc. v. Does 1-21	3:11-cv-02258	ND CA	5/6/11
MCGIP, LLC v. Does 1-21	4:11-cv-01783	ND CA	4/12/11
Hard Drive Productions, Inc. v. Does 1-21	4:11-cv-00059	SD IN	5/20/11
Hard Drive Productions, Inv. v. Does 1-20	1:11-cv-22208	SD FL	6/17/11
AF Holdings LLC v. Does 1-20	3:11-cv-00491	WD KY	8/31/11
Millennium TGA, inc. v. Does 1-21	5:11-cv-01739	ND CA	4/8/11
Boy Racer Inc. v. Does 1-23	4:11-cv-00070	SD IN	6/14/11
First Time Videos LLC v. Does 1-23	1:11-cv-05417	ND IL	8/10/11
Boy Racer Inc. V. Does 1-22	1:11-cv-02984	ND IL	5/4/11
MCGIP, LLC v. Does 1-24	1:11-cv-04488	ND IL	7/1/11
Hard Drive Productions Inc. v. Does 1-25	1:11-cv-03864	ND IL	6/7/11
Openmind Solutions, Inc. v. Does 1-2,925	3:11-cv-00092	SD IL	2/2/11
MCGIP, LLC v. Does 1-24	1:11-cv-02985	ND IL	5/4/11
Hard Drive Productions, Inc. v. Does 1-24	1:11-cv-02829	ND IL	4/27/11
MCGIP LLC v. Does 1-26	5:11-cv-03679	ND CA	7/27/11
Hard Drive Productions, Inc. v. Does 1-27	1:11-cv-03863	ND IL	6/7/11
First Time Videos LLC v. Does 1-27	1:11-cv-02890	ND IL	4/29/11
Pacific Century International Ltd, v. Does 1-129	5:11-cv-03681	ND CA	7/27/11
First Time Videos LLC v. Does 1-28	1:11-cv-02982	ND IL	5/4/11
MCGIP LLC v. Does 1-30	5:11-cv-03680	ND CA	7/27/11
Hard Drive Productions, Inv. v. Does 1-130	4:11-cv-03826	ND CA	8/3/11
AF Holdings LLC v. Does 1-29	0:11-cv-01794	D MN	7/6/11
Hard Drive Productions, Inc. v. Does 1-30	1:11-cv-22102	SD FL	6/9/11
Pacific century International LTD v. Does 1-31	1:11-cv-09064	ND IL	12/21/11
Hard Drive Productions, Inv. v. Does 1-33	4:11-cv-03827	ND CA	8/3/11
Hard Drive Productions, Inv. v. Does 1-32	1:11-cv-22206	SD FL	6/17/11
MCGIP, LLC v. Does 1-32	1:11-cv-22210	SD FL	6/17/11
Pacific Century International LTD v. Does 1-34	1:11-cv-03857	ND IL	6/7/11
Hard Drive Productions, Inc. v. Does 1-35	1:11-cv-03866	ND IL	6/7/11
Boy Racer Inc v. Does 1-34	1:11-cv-23035	SD FL	8/23/11
AF Holdings LLC v. Does 1-135	4:11-cv-03336	ND CA	7/7/11
Bubble Gum Productions, LLC v. Does 1-37	1:12-cv-00595	ND IL	1/26/12
First Time Videos LLC v. Does 1-37	4:11-cv-01675	ND CA	4/6/11
Openmind Solutions, Inc. v. Does 1-39	3:11-cv-03311	ND CA	7/6/11
First Time Videos LLC v. Does 1-541	1:11-cv-02031-RLW	DC	11/15/11
Hard Drive Productions, Inc. v. Does 1-42	3:11-cv-01956	ND CA	4/22/11
First Time Videos LLC v. Does 1-43	1:11-cv-09066	ND IL	12/21/11
MCGIP, LLC v. Does 1-44	1:11-cv-03098	ND IL	5/9/11
Pacific Century International LTD v. Does 1-44	1:11-cv-04825	ND IL	7/18/11
Hard Drive Productions, Inc. v. Does 1-44	1:11-cv-02828	ND IL	4/27/11
Pink Lotus Entertainment LLC v. Does 1-46	5:11-cv-02263	ND CA	5/6/11
First Time Videos LLC v. Does 1-46	3:11-cv-03822	ND CA	8/3/11
Hard Drive Productions, Inc v. Does 1-46	3:11-cv-01959	ND CA	4/22/11
Pacific Century International, LTD v. Does 1-48	3:11-cv-03823	ND CA	8/3/11
Hard Drive Productions, Inc. v. Does 1-48	3:11-cv-01957	ND CA	4/22/11
Hard Drive Productions, Inc. v. Does 1-48	1:11-cv-09062	ND IL	12/21/11
MCGIP, LLC v. Does 1-49	5:11-cv-01801	ND CA	4/13/11
MCGIP, LLC v. Does 1-149	4:11-cv-02331	ND CA	5/11/11
Hard Drive Productions, Inc. v. Does 1-51	1:11-cv-05414	ND IL	8/10/11
Boy Racer Inc v. Does 2-52	5:11-cv-02834	ND CA	6/14/11
Boy Racer Inc. v. Does 1-52	5:11-cv-02329	ND CA	5/11/11
Hard Drive Productions, Inc. v. Does 1-53	3:11-cv-02330	ND CA	5/11/11
Pink Lotus Entertainment LLC v. John Does 1-53	1:11-cv-22103	SD FL	6/9/11

MCGIP LLC v. Does 1-55	3:11-cv-03312	ND CA	7/6/11
Hard Drive Productions, Inv. v. Does 1-55	1:11-cv-02798	ND IL	4/27/11
Hard Drive Productions, Inc. v. Does 1-58	4:11-cv-02537	ND CA	5/25/11
AF Holdings LLC v. Does 1-1,058	1:12-cv-00048	DC	1/11/12
Boy Racer Inc v. Does 1-60	3:11-cv-01738	ND CA	4/8/11
AF Holdings LLC v. Does 1-62	1:11-cv-00593	SD OH	8/26/11
AF Holdings LLC v. Does 1-162	1:11-cv-23036	SD FL	8/23/11
First Time Videos LLC v. Does 1-63	1:11-cv-03837	ND IL	6/6/11
MCGIP, LLC v. Does 1-1,164	1:10-cv-07675	ND IL	12/2/10
Hard Drive Productions, Inv. v. Does 1-166	5:11-cv-03682	ND CA	7/27/11
Openmind Solutions, Inc. v. Does 1-565	1:11-cv-01883	DC	10/25/11
Hard Drive Productions, Inc.v. Does 1-66	5:11-cv-03005	ND CA	6/17/11
Boy Racer Inc v. Does 2-71	5:11-cv-02833	ND CA	6/14/11
Boy Racer Inc. v. Does 1-71	5:11-cv-01958	ND CA	4/22/11
Heartbreaker Productions, Inc. v. Does 1-71	1:11-cv-02860	ND IL	4/28/11
Boy Racer Inc v. Does 1-73	3:11-cv-02534	ND CA	5/25/11
First Time Videos LLC v. Does 1-76	1:11-cv-03831	ND IL	6/6/11
Hard Drive Productions, Inc. v. Does 1-80	5:11-cv-02535	ND CA	5/25/11
Bubble Gum Productions, LLC v. Does 1-80	1:12-cv-20367	SD FL	1/30/12
Hard Drive Productions, Inv. v. Does 1-84	5:11-cv-03648	ND CA	7/26/11
Pacific Century International LTD v. Does 1-87	3:11-cv-02915	ND CA	6/14/11
First Time Videos LLC v. Does 1-186	3:11-cv-03310	ND CA	7/6/11
Hard Drive Productions, Inc v. Does 1-87	3:11-cv-02333	ND CA	5/11/11
Hard Drive Productions, Inc v. Does 1-188	3:11-cv-01566	ND CA	3/31/11
Hard Drive Productions, Inc v. Does 1-87	5:11-cv-03004	ND CA	6/17/11
Hard Drive Productions, Inv. v. Does 1-90	5:11-cv-03825	ND CA	8/3/11
First Time Videos LLC v. Does 1-294	3:11-cv-02916	ND CA	6/14/11
Hard Drive Productions, Inv. v. Does 1-1,495	1:11-cv-01741	DC	9/27/11
AF Holdings LLC v. Does 1-96	3:11-cv-03335	ND CA	7/7/11
AF Holdings LLC v. Does 1-97	4:11-cv-03067	ND CA	6/21/11
Boy Racer Inc. v. Does 1-98	3:11-cv-02536	ND CA	5/25/11