

FILED
UNITED STATES DISTRICT COURT
DENVER, COLORADO

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

AUG 27 2012

GREGORY C. LANGHAM
CLERK

Civil Action No. 1:12-cv-00886 *MEH*

Malibu Media, LLC,
Plaintiff,

v.

Jeff Fantalis and Bruce Dunn
Defendants.

DEFENDANT'S SECOND AMENDED ANSWER AND COUNTERCLAIM

Defendant, Jeff Fantalis, by way of Answer to the complaint of Malibu Media, LLC (the "Plaintiff"), says:

Introduction¹

1. Defendant denies that Plaintiff has any cause(s) of action against Defendant under the United States Copyright Act of 1976 or under any other legislation or at common law.
2. Denied in its entirety, including the footnote.
3. Defendant has no personal knowledge of any of the movies referred to by Plaintiff.
4. Denied.

¹ The headings of the Complaint are used in this Answer solely for the convenience of the Court. Defendant does not admit any of Plaintiff's allegations by such use.

Jurisdiction and Venue

5. Defendant denies that Plaintiff has any cause of action against him; however, he admits that this court has subject matter jurisdiction over matters involving federal questions and copyrights.
6. Defendant denies the allegations of this paragraph. Even if the IP address in question (184.96.0.193) was associated with the high-speed internet router located in Defendant's home on or about January 14, 2012, that fact would not give rise to jurisdiction over the Defendant's person. An IP address is not a person but a designation assigned to a piece of technology, which can be accessed by multiple individuals; in addition, in a process commonly known as "spoofing" an IP address can be stolen or misused as follows: other devices can be configured with the same IP address or an individual can utilize technology to make his or her own IP address to appear to be another IP address.
7. Defendant denies the allegations of this paragraph, except to admit that he is a resident of the City of Louisville, County of Boulder, and State of Colorado. Defendant was not served with a Summons at the time of service of the Complaint, as required by the Federal Rules of Civil Procedure. For all of these reasons, Plaintiff has failed to plead facts from which a reasonable trier of fact could conclude that this Court has personal jurisdiction over Defendant, or that venue is properly laid in this district. Defendant has no personal knowledge as to relevant information regarding the other defendants in this matter.

Parties

8. Defendant has no personal knowledge of these facts and can neither confirm nor deny and leaves Plaintiff to its proofs.

9. Defendant admits that he is a resident of the state of Colorado. Defendant has no knowledge as to the IP address provided by Qwest/CenturyLink.
10. Defendant has no personal knowledge of these facts and can neither confirm nor deny and leaves Plaintiff to its proofs.
11. Defendant has no personal knowledge of these facts and can neither confirm nor deny and leaves Plaintiff to its proofs.
12. Defendant denies the allegations of this paragraph. Plaintiff's definition is incomplete and misleading.
13. Defendant denies the allegations of this paragraph.

Joinder

14. Defendant denies the allegations of this paragraph. Among other reasons, Plaintiff's Exhibit C demonstrates that the individual Defendants could not have, in fact, been involved in "the exact same torrent file" or having "act[ed] in concert with each other" as alleged by the Plaintiff, as Exhibit C asserts infringement by the individual Defendants as having occurred on three distinct and separate dates. The factual situations of the three defendants are individual, separate, distinct and unique. Their legal defenses and counterclaims are similarly going to be individual, separate, distinct and unique.

Factual Background

I. Plaintiff Owns The Copyright to a Motion Picture

15. Defendant has no personal knowledge of these allegations and can neither confirm nor deny, and leaves Plaintiff to its proofs.
16. Defendant has received a copy of the alleged copyright registrations as Exhibit B.

17. Defendant denies this paragraph to the extent that it alleges copyright infringement or any other unlawful or illegal conduct by the Defendant. Among all other reasons stated herein, Defendant was not at home on the date and at the time of the activity alleged by Exhibit C. Defendant also disputes the validity of Plaintiff's alleged copyrights as a matter of law.

II. Defendants Used BitTorrent To Infringe Plaintiff's Copyright

18. Defendant leaves Plaintiff to its proofs with regard to this description of BitTorrent technology. Defendant has received a copy of Exhibit D.

19. Defendant leaves Plaintiff to its proofs with regard to this description of BitTorrent technology.

A. Each Defendant Installed a BitTorrent Client onto his or her Computer

20. Defendant denies the allegations of this paragraph.

21. Defendant leaves Plaintiff to its proofs with regard to this description of BitTorrent technology.

22. Defendant leaves Plaintiff to its proofs with regard to this description of BitTorrent technology.

B. The Initial Seed, Torrent, Hash and Tracker

23. Defendant leaves Plaintiff to its proofs with regard to this description of BitTorrent technology.

24. Defendant leaves Plaintiff to its proofs with regard to this description of BitTorrent technology.

25. Defendant leaves Plaintiff to its proofs with regard to this description of BitTorrent technology.

26. Defendant leaves Plaintiff to its proofs with regard to this description of BitTorrent technology.

27. Defendant leaves Plaintiff to its proofs with regard to this description of BitTorrent technology.

28. Defendant leaves Plaintiff to its proofs with regard to this description of BitTorrent technology.

29. Defendant leaves Plaintiff to its proofs with regard to this description of BitTorrent technology and its relation to Plaintiff's alleged copyrighted Works.

30. Defendant leaves Plaintiff to its proofs with regard to this description of BitTorrent technology.

C. Torrent Sites

31. Defendant leaves Plaintiff to its proofs with regard to this description of BitTorrent technology.

32. Defendant denies the allegations of this paragraph.

D. Uploading and Downloading Works Through a BitTorrent Swarm

33. Defendant leaves Plaintiff to its proofs with regard to this description of BitTorrent technology.

34. Defendant leaves Plaintiff to its proofs with regard to this description of BitTorrent technology and its relation to Plaintiff's alleged copyrighted Works.

35. Defendant leaves Plaintiff to its proofs with regard to this description of BitTorrent technology and its relation to Plaintiff's alleged copyrighted Works.

36. Defendant leaves Plaintiff to its proofs with regard to this description of BitTorrent technology.

37. Defendant denies the allegations of this paragraph. In addition, Plaintiff's own Exhibit C demonstrates that the individual Defendants could not have been part of the same "swarm" as described by the Plaintiff.

38. Defendant leaves Plaintiff to its proofs with regard to this description of BitTorrent technology and its relation to Plaintiff's alleged copyrighted Works.

39. Defendant denies the allegations of this paragraph with regard to any alleged activity by the Defendant. As to the general process of participating in a BitTorrent, Defendant leaves Plaintiff to its proofs.

E. Plaintiff's Computer Investigators Identified Each of the Defendants' IP Addresses as Participants in a Swarm That Was Distributing Plaintiff's Copyrighted Works

40. Defendant has no personal knowledge of these facts and can neither confirm nor deny, and leaves Plaintiff to its proofs. Upon information and belief, IPP will receive a portion of any judgment or settlement obtained by Plaintiff from these legal proceedings and as such has an improper financial interest in this litigation that taints its potential testimony.

41. Defendant has no personal knowledge of these facts and can neither confirm nor deny, and leaves Plaintiff to its proofs. Upon information and belief, IPP will receive a portion of any judgment or settlement obtained by Plaintiff from these legal proceedings and as such has an improper financial interest in this litigation that taints its potential testimony.

42. Defendant has no personal knowledge of these facts and can neither confirm nor deny, and leaves Plaintiff to its proofs. Upon information and belief, IPP will receive a portion of any judgment or settlement obtained by Plaintiff from these legal proceedings and as such has an improper financial interest in this litigation that taints its potential testimony.

43. Defendant denies the allegations of this paragraph including subparts (A) and (B).

44. Defendant denies the allegations of this paragraph.

45. Defendant has no personal knowledge of these facts and can neither confirm nor deny, and leaves Plaintiff to its proofs.

46. Defendant has no personal knowledge of these facts and can neither confirm nor deny, and leaves Plaintiff to its proofs.

Miscellaneous

47. Defendant has no personal knowledge of these facts and can neither confirm nor deny, and leaves Plaintiff to its proofs.
48. Defendant has no personal knowledge of these facts and can neither confirm nor deny, and leaves Plaintiff to its proofs.

COUNT I

Direct Infringement Against Defendants

49. Defendant's denials and statements in response to paragraphs 1-48 are hereby incorporated as though fully set forth herein.
50. Defendant has no personal knowledge of these facts and can neither confirm nor deny, and leaves Plaintiff to its proofs. Defendant also disputes the validity of Plaintiff's alleged copyrights as a matter of law.
51. Defendant denies the allegations of this paragraph.
52. Defendant has no knowledge as to the Plaintiff's explicit authorization or permission as to any downloads of the Works in question. However, by uploading them to the internet as they allege they have done in this Complaint, they implicitly authorized public access, downloading, copying, distributing, and other use of their Works. Defendant denies having participated in any activity by which Plaintiff's alleged copyrights were infringed.
53. Defendant denies the allegations of this paragraph, including subparagraphs (A) through (D).
54. Defendant denies the allegations of this paragraph.
55. Defendant denies the allegations of this paragraph. Defendant has not engaged in any activity that would harm the Plaintiff or in any way give rise to a cause of action as claimed herein or in any other manner.

WHEREFORE, Defendant respectfully requests that the Court:

- (A) Find that the Plaintiff's Complaint is entirely without merit; and
- (B) Immediately dismiss Plaintiff's Complaint, with prejudice; and
- (C) Award Defendant his reasonable fees and costs of suit; and
- (D) Grant Defendant such other and further relief as the Court may deem equitable and just.

COUNT II

Contributory Infringement Against Defendants

56. Defendant's denials and statements in response to paragraphs 1-55 are hereby incorporated as though fully set forth herein.

57. Defendant has no personal knowledge of these facts and can neither confirm nor deny, and leaves Plaintiff to its proofs. Defendant also disputes the validity of Plaintiff's alleged copyrights as a matter of law.

58. Defendant denies the allegations of this paragraph.

59. Defendant denies the allegations of this paragraph.

60. Defendant has no knowledge as to the Plaintiff's explicit authorization or permission as to any downloads of the Works in question. However, by uploading them to the internet as they allege they have done in this Complaint, they implicitly authorized public access, downloading, copying, distributing, and other use of their Works. Defendant denies having participated in any activity by which Plaintiff's alleged copyrights were infringed.

61. Defendant denies the allegations of this paragraph.

62. Defendant denies the allegations of this paragraph.

63. Defendant denies the allegations of this paragraph.

64. Defendant denies the allegations of this paragraph.

65. Defendant denies the allegations of this paragraph. Defendant has not engaged in any activity that would harm the Plaintiff or in any way give rise to a cause of action as claimed herein or in any other manner.

WHEREFORE, Defendant respectfully requests that the Court:

- (A) Find that the Plaintiff's Complaint is entirely without merit; and
- (B) Immediately dismiss Plaintiff's Complaint, with prejudice; and
- (C) Award Defendant his reasonable fees and costs of suit; and
- (D) Grant Defendant such other and further relief as the Court may deem equitable and just.

AFFIRMATIVE DEFENSES

**FIRST AFFIRMATIVE DEFENSE
(Failure to State a Claim for Relief)**

Plaintiff has failed to state a claim upon which relief may be granted.

**SECOND AFFIRMATIVE DEFENSE
(Statute of Limitations)**

Plaintiff's claims are barred by the applicable statute of limitations.

**THIRD AFFIRMATIVE DEFENSE
(Lack of Subject Matter Jurisdictional Failure to Register)**

Plaintiff's claims are barred for a lack of subject matter jurisdiction because it lacks valid copyright registrations for the intellectual property rights asserted or has not properly or timely registered its works.

**FOURTH AFFIRMATIVE DEFENSE
(Lack of Originality)**

Plaintiff's works lack originality and are thus not protectable by copyright.

**FIFTH AFFIRMATIVE DEFENSE
(Invalidity or Unenforceability of Copyright)**

Plaintiff's copyrights are invalid and/or unenforceable.

**SIXTH AFFIRMATIVE DEFENSE
(Fair Use)**

Plaintiff's claims are barred by the doctrine of fair use.

**SEVENTH AFFIRMATIVE DEFENSE
(Estoppel)**

Plaintiff's claims are barred by estoppel.

**EIGHTH AFFIRMATIVE DEFENSE
(Unclean Hands)**

Plaintiff's claims are barred by the doctrine of unclean hands.

**NINTH AFFIRMATIVE DEFENSE
(Waiver)**

Plaintiff's claims are barred by waiver.

**TENTH AFFIRMATIVE DEFENSE
(Authorized Use)**

Plaintiff authorized, impliedly or explicitly, Defendant's allegedly infringing use of its works, and Plaintiff's claims are therefore barred by the doctrine of implied license.

**ELEVENTH AFFIRMATIVE DEFENSE
(License, Consent, and Acquiescence)**

Plaintiff's claims are barred by Plaintiff's license, consent, and acquiescence to Defendant.

**TWELFTH AFFIRMATIVE DEFENSE
(Failure to Mitigate Damages)**

To the extent Plaintiff suffered any damages, which Defendant expressly denies; Plaintiff has failed to take the steps necessary to mitigate the damages sustained.

**THIRTEENTH AFFIRMATIVE DEFENSE
(Forfeiture or Abandonment)**

Plaintiff's claims are barred to the extent it has forfeited or abandoned its intellectual property.

**FOURTEENTH AFFIRMATIVE DEFENSE
(Misuse of Copyright)**

Plaintiff's claims are barred by the doctrine of misuse of copyright.

**FIFTEENTH AFFIRMATIVE DEFENSE
(Innocent Intent)**

Plaintiff's claims are barred, in whole or in part, because Defendant conduct was in good faith and with non-willful intent, at all times.

**SIXTEENTH AFFIRMATIVE DEFENSE
(Unconstitutionally Excessive Damages)**

Plaintiff's claims are barred because statutory damages sought are unconstitutionally excessive and disproportionate to any actual damages that may have been sustained in violation of the Due Process clause.

**EIGHTEENTH AFFIRMATIVE DEFENSE
(Statutory Damages)**

Plaintiff's claims for statutory damages under 17 U.S.C. § 504 is barred because Plaintiff's copyright registrations were not made within three months after the first publication of the allegedly infringing works, as required by 17 U.S.C. § 412.

**NINETEENTH AFFIRMATIVE DEFENSE
(Injunctive Relief)**

Plaintiff is not entitled to injunctive relief because any alleged injury to Plaintiff is not immediate or irreparable, and Plaintiff has an adequate remedy at law.

Pursuant to FRCP 11, as amended, all possible affirmative defenses may not have been alleged herein insofar as sufficient facts were not available after reasonable inquiry upon the filing of Defendant's Answer, and therefore Defendant reserves the right

to amend its answer to allege additional affirmative defenses, if subsequent investigation so warrants.

COUNTERCLAIM

Defendant, Jeff Fantalis, by way of counterclaim against the Plaintiff, Malibu Media, LLC, says:

1. Defendant is an individual residing in the State of Colorado.
2. This court has jurisdiction over Plaintiff, Malibu Media, LLC, because Plaintiff has availed itself of this court to pursue an action against the Defendant, and this is also therefore the proper venue. This court has subject matter jurisdiction due to diversity and pursuant to the Declaratory Judgment Act, 28 U.S.C.2201, 2202.

FACTS COMMON TO ALL COUNTS

Parties

3. Defendant is a 46 year old married man with two children. He has never downloaded a pornographic film or any other type of film through a BitTorrent. The only films Defendant has ever downloaded are through the Netflix service for which he and his wife pay a monthly service fee.
4. Defendant has no knowledge of any other person or entity using his computer, router or modem to download a pornographic film.
5. Defendant never authorized another person or entity to use his computer, router or modem to download a pornographic film.

6. Defendant never benefited from, nor authorized, either explicitly nor implicitly, any person or entity to use his computer, router or modem to download a pornographic film.
7. Upon information and belief, Plaintiff, Malibu Media LLC, is either a producer, distributor and purveyor of pornography, or it is a shell corporation created solely and expressly for the purpose of purchasing copyrights to pornographic films in order to initiate lawsuits against internet users and collect settlements from them. It is unclear at this stage of the litigation which type of company Plaintiff is; however, upon information and belief, it appears to be the latter. An internet search of "Malibu Media LLC" turns up nothing but these lawsuits for copyright infringement. There is no corporate website, no advertising or marketing materials, and, perhaps most important, no legitimate means for an individual to purchase the films that Plaintiff claims to be trying to protect from infringement.
8. To the extent that Plaintiff holds any copyrights, Defendant is informed and believes that Plaintiff purchased the rights to the pornographic films only after it discovered that the films had been the subject of infringing behavior for the sole purpose of initiating lawsuits such as described herein.
9. While Plaintiff asserts that this action, and by extension the dozens of other identical cases filed by Plaintiff in Colorado alone, are being filed in order to protect its copyrights in these pornographic films, upon information and belief, this case and all the others like it are part of a series of hundreds of litigations initiated over the past several years by this Plaintiff and other pornography companies. Upon information and belief, to date, not a single one of the hundreds of cases filed by Plaintiff and similarly situated producers of pornographic materials have ever been brought to trial.

10. Plaintiff, like the other pornography company plaintiffs, has engaged in a deliberate, intentional and systematic course of action, knowingly relying on often false and inaccurate data, the purpose of which is not to protect their copyrights, but rather to embarrass, shame and coerce individuals who use the internet into paying a settlement in order to avoid litigation, regardless of whether those individuals have actually done anything wrong. The Plaintiff and the other pornography companies are blatantly misusing the power of the Federal Court system as a tool in their scheme.
11. This wrongful course of action has been well documented in the media (see, for example, **Exhibit A**, www.usnews.com article of February 2, 2012, "Porn Companies File Mass Piracy Lawsuits": <http://www.usnews.com/news/articles/2012/02/02/porn-companies-file-mass-piracy-lawsuits-are-you-at-risk>; and in a case in the U.S. District Court, Eastern District of New York, it has been called a "nationwide blizzard." *In Re BitTorrent Adult Film Copyright Infringement Cases*, 2:11-cv-03995, 12-1147, 12-1150, and 12-1154, Order and Report and Recommendation dated May 1, 2012 at p. 2.²
12. Upon information and belief, the principal and or principals of Plaintiff Malibu Media LLC are also the principal(s) of another pornography company known as Click Here LLC which owns the pornographic website X-Arts.com. The registered address of Click Here LLC is 31356 Broad Beach Road, Malibu, California 90265, which is the same address alleged for Malibu Media LLC. Complaint ¶¶ 8. The agent for service of process, Brigham Field, is the same for Malibu Media LLC and for Click Here LLC.
13. Plaintiff's counsel of record, Jason A. Kotzker, Esq., represents Plaintiff in multiple BitTorrent copyright infringement litigations which are substantially identical to this

² It is notable that in two out of the four cases to which that order applies, the plaintiff is Malibu Media, LLC, and in three of the four cases, the attorney of record is Jason Kotzker, Esq., counsel for Plaintiff herein.

case here in Colorado and also represents Plaintiff in multiple substantially identical BitTorrent litigations in New York state. Jason A. Kotzker, Esq., also represents another pornography company in these types of cases, Patrick Collins, Inc., both in Colorado and New York. Upon information and belief, Patrick Collins, Inc., and yet another one of these pornography companies involved in this blizzard of law suits, Raw Films, Ltd., are substantially the same companies, owned and operated by the same individuals and represented by the same attorneys.³ In this way, small groups of individuals are creating multiple companies behind which they can hide while executing a nationwide money-making agenda.

The For-Profit Business Model of the “Copyright Trolls”

14. These pornography companies who are pursuing infringement lawsuits as a for-profit business model have become known as “copyright trolls.”
15. The first step in the “copyright troll” business is the collection of IP (internet protocol) addresses. A third party investigator or “harvester” gathers and collects information regarding IP addresses that are allegedly transmitting a copyrighted work via BitTorrent. In some cases, the investigators are hired by the pornography companies; in other cases, the investigators contact the pornography companies to alert them to this potential source of revenue. See, **Exhibit B, Business Proposal by Anti-Piracy Management Company LLC (APMC)** which presents this business model in detail. Upon information and belief, APMC operates in a substantially similar if not identical fashion as IPP Ltd., the “harvester” used by Plaintiff in this case. APMC, an IP “harvesting” firm, offers to collect IP “evidence” which is then “sent to the law firm

³ Tobias Fieser of IPP, Ltd., who filed a Declaration in *Malibu Media v. John Does 1-30*, 1:12-cv-00402, in support of Plaintiff’s Motion for expedited discovery, has filed substantially identical Declarations in support of substantially identical Motions for expedited discovery by K-Beech and Patrick Collins in other substantially identical litigations. See, e.g., *K-Beech, Inc. v. John Does 1-18*, E.D. Mi. Case No. 11-cv-15226; *Patrick Collins, Inc. v. John Does 1-26*, W.D.N.C. Case No. 11-cv-0394.

in the jurisdiction in question so it can prepare an application to court for a disclosure order against the ISPs. Then the names and address (sic) relating to the IP addresses identified can be acquired... The infringers are then written to and a demand for payment of damages and costs is made..." Of great interest is the concluding sentence of the third paragraph on the first page: **"If payment is not forthcoming, proceedings are then commenced to obtain an order from the court, which can then be enforced against the infringer, if necessary, and also sent to other infringers, *pour encourager les autres*. (in order to encourage the others)."** (italics in original, emphasis added). This sentence could not be more clear: it is part of the business plan to utilize court proceedings against one individual to threaten and intimidate the others.

16. Indeed, that is exactly what has happened in this case here in Colorado: as will be demonstrated below, Plaintiff has filed over 30 of cases against approximately 500 Doe defendants and only twelve cases against actual named defendants, mostly after Defendant countersued. Clearly, Defendant is being used as an exemplar "*pour encourager les autres*" in the words of APMC's business proposal. Defendant's case can be used as an additional threat to hold over other Does – "look what happened to this guy when he didn't settle." The term "to encourage the others" is shockingly disingenuous, when what it really means is to hold a club over their heads.

17. APMC's proposal goes on to say that the monetary amount claimed should not be excessive: "Ordinarily, we usually claim from each infringer an amount (depending on the copyright work involved) which is not unduly excessive, the aim being for the infringer to experience receiving **an expensive, but affordable, 'parking ticket'** for his or her misdemeanor." Exhibit B, p. 1, para. 4 (emphasis added). APMC happily asserts a 25% success rate after the initial demand letter and notes, "[u]p to a further 10% tend to pay up once they have had their questions answered." APMC notes that

“the deterrent effect (and revenue collected) can be quite substantial.” APMC also brags about its partner law firms’ success at obtaining court orders, a key element to the success of this scheme. This for-profit business model is further complicated by the fact that the pornography company’s attorney is paid a portion of any settlements received, establishing a champertous relationship ripe for abuse against mostly defenseless *pro se* defendants who would likely be bankrupted by even the most minimal legal defense.

18. With such prospects for success, the pornography company rarely leaves the infringement to chance. Frequently, the plaintiff sets out to actively draw infringers to its films, and does so by uploading a digital file containing its films to the internet. This digital file planted on the internet is known as a “honeypot.”
19. Once this file becomes involved in a BitTorrent download, the pornography company, through its investigator, can track other IP addresses that may or may not be involved in the BitTorrent. It is well known that the kind of tracking technology commonly used by such companies is not reliable and may result in “false positives” showing infringement by devices such as printers, routers or telephones which are incapable of performing the download; *see, e.g., Exhibit C, Piatek, Kohno, and Krishnamurthy, Challenges and Directions for Monitoring P2P Filesharing Networks, or Why My Printer Received a DMCA Takedown Notice, http://dmca.cs.washington.edu/dmca_hotsec08.pdf*.
20. Defendant alleges that upon information and belief, Plaintiff follows this for-profit litigation business model wherein the IP harvesting company creates the “honeypot” by uploading the Plaintiff’s work and is in fact a financially interested party.
21. Defendant also alleges that upon information and belief this for-profit litigation business model is nearly exclusively attorney driven, with minimal or no involvement from the actual copyright holder.

22. Upon information and belief, counsel in this case takes direction not from the copyright holder but from another attorney, namely M. Keith Lipscomb who in reality is acting as the *de facto* plaintiff in an effort to initiate legal action against tens of thousands of individuals with the sole purpose of generating a significant profit from high pressure out-of-court settlements as will be discussed below.
23. Defendant alleges that such a relationship amounts to acts of champerty and barratry which constitute an abuse of the judicial process.
24. Plaintiff allegedly utilized a company called IPP, Ltd., to collect IP addresses and hashtag information regarding the alleged infringement of the Works for which it claims it copyrights. (Significantly, Plaintiff did not provide any documentation of the manner in which IPP, Ltd., collected the information it gathered with the Complaint it filed against Defendant.)
25. Upon information and belief, IPP, Ltd., is substantially the same as a German company called Guardaley Ltd. (a/k/a GuardaLey). Upon information and belief, IPP, Ltd., is owned, in whole or in part, by Guardaley or by the individuals who own Guardaley, and is operated by the same or substantially the same individuals. Upon information and belief, IPP, Ltd., utilizes the same technology as Guardaley or substantially similar technology to gather IP addresses.
26. The flaws and unreliability of Guardaley's IP address harvesting technology have been established in the German law courts. Guardaley was sued by Baumgarten Brandt, a German law firm that had a contract with Guardaley whereby Guardaley would provide the law firm with IP addresses of potential BitTorrent copyright infringers. Baumgarten Brandt sued Guardaley when they discovered that Guardaley was aware of flaws in their IP addresses collection technology but chose not to disclose those flaws to Baumgarten Brandt.

27. In May of 2011, the State Court of Berlin found that, when identifying infringers, Guardaley (1) operated a “honeypot”; (2) identified as “infringers” IP addresses that merely “inquired” about a file, whether or not a file was actually shared; (3) identified as “infringers” IP addresses that neither uploaded nor downloaded any files; and (4) did not identify how it identified each IP address, so there was no way to distinguish actual infringing IP addresses from those that did not engage in infringing activity. See, **Exhibit D**, court filing by Baumgarten Brandt from State Court of Berlin, and **Exhibit E**, demonstrating the flaws in Guardaley’s technology.
28. Once IP addresses are collected, the company files a Complaint in Federal Court claiming that hundreds or thousands of individuals have illegally downloaded their copyright protected materials. The Complaint identifies the defendants as “John Does” and states that they are subscribers to certain IP addresses. The Complaint further avers unequivocally that the subscriber to the IP address is the infringer who illegally downloaded the copyrighted pornography. This statement is without foundation in the law or in common sense, and yet the pornography companies are counting on the possibility that some judges would not be technologically savvy order to accomplish their goals.⁴ (In this case, Plaintiff filed its “John Doe” complaint making these claims on February 15, 2012, as *Malibu Media v. John Does 1-30*, Civil Action No. 1:12-cv-00402-WYD-MEH. Note that Defendant was never served with the Complaint in that matter.)
29. The plaintiff company further represents to the court in its Complaint that the Doe defendants are all guilty of downloading plaintiff’s copyrighted works via BitTorrent; that the acts of copyright infringement occurred using each of the Doe defendants’ IP

⁴ Magistrate Judge Gary R. Brown, for one, was not fooled: “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.” In Re BitTorrent Adult Film, supra, 2:11-cv-03995, May 1, 2012, at p. 6.

addresses; and that the ISP can correlate or connect the IP address to the Doe defendant's – and therefore, the infringer's – true identity. (*Malibu Media v. Does 1-30*: Complaint para. 11, 35, 42-44, 51, 54,58-64). The plaintiff makes these statements despite the fact that, at this point, the identity – and therefore, the conduct, actions and intent – of any of the defendants is entirely unknown to the plaintiff company. Plaintiff was or should have been aware of these facts at the time it filed the action against the Doe defendants, including Defendant, in this case on February 15, 2012.

30. Furthermore, the plaintiff company makes these statements even though it knew or should have known that the IP addresses it identifies in the Complaint do not represent people, nor can they even be said with certainty to be computers; in fact, an IP address may be assigned to or attached to many different kinds of electronic devices, such as wireless routers, video games, printers, or telephones, or indeed any other device capable of operation through a modem. Numerous courts have definitively affirmed this principle. See, e.g., *In Re BitTorrent Adult Film*, supra, 2:11-cv-03995, May 1, 2012, at p. 6; *Malibu Media LLC v. John Does 1-10*, 2:12-cv-3623, Order, June 27, 2012. Plaintiff was or should have been aware of these facts at the time it filed the action against the Doe defendants, including Defendant, in this case on February 15, 2012.

31. There are many ways in which a subscriber can be misidentified as an infringer without participating in any infringing behavior, including but not limited to:

a. Some members of a swarm simply and automatically pass on routing information to other clients, and never possess even a bit of the movie file;⁵

⁵ Sengupta, S. et al., Peer-to-Peer Streaming Capacity, *IEEE Transactions on Information Theory*, Vol. 57, Issue 8, pp. 5072-5087, at 5073 (Prof. Helmut Bolcski, ed., 2011) (“A [BitTorrent] user may be the source, or a receiver, or a helper that serves only as a relay.”).

- b. A client requesting a download can substitute another IP address for its own to a Bittorrent tracker;⁶
- c. A user can misreport its IP address when uploading a torrent file;⁷
- d. A user in the network path between the user monitoring IP address traffic and the Bittorrent tracker can implicate another IP address;⁸
- e. Malware on a computer can host and distribute copyrighted content without knowledge or consent;⁹
- f. There are reliability issues with using IP addresses and timestamps to identify the correct party;¹⁰
- g. If a subscriber has dynamic IP addressing through its website host, it is sharing an IP address with several other subscribers;¹¹ or
- h. Anyone with wireless capability can use a subscriber's "wi-fi" network to access the Internet, giving the impression that it is the subscriber who is infringing.¹²

⁶ Michael Piatek et al., *Challenges and Directions for Monitoring P2P File Sharing Networks—or—Why My Printer Received a DMCA Takedown Notice*, 3 (2008), http://dmca.cs.washington.edu/uwcse_dmca_tr.pdf (Exhibit C). See also, "IP address spoofing" http://en.wikipedia.org/wiki/IP_address_spoofing (Last visited August 2, 2012) (the term IP address "spoofing" refers to the creation of a forged IP address with the purpose of concealing the user's identity or impersonating another computing system.). Specifically, the article concludes: "[W]e find that it is possible for a malicious user (or buggy software) to implicate (frame) seemingly any network endpoint in the sharing of copyrighted materials. We have applied these techniques to frame networked printers, a wireless (non-NAT) access point, and an innocent desktop computer, all of which have since received DMCA takedown notices but none of which actually participated in any P2P networks."

⁷ [Ibid.](#)

⁸ [Ibid.](#)

⁹ [Ibid.](#)

¹⁰ "Web hosting service" http://en.wikipedia.org/wiki/Web_hosting_service (Last visited August 2, 2012).

¹¹ Piatek, *supra*. ("When IP addresses are assigned dynamically, reassignment of an IP address from an infringing user to an innocent user can cause the behavior of the infringing user to be attributed to the innocent user. Because the monitoring client (copyright holder) records information from the tracker of the Bittorrent client, the information can quickly become inaccurate and will not implicate the correct user.")

¹² Carolyn Thompson writes in an MSNBC article of a raid by federal agents on a home that was linked to downloaded child pornography. The identity and location of the subscriber were provided by the ISP. The desktop computer, iPhones, and iPads of the homeowner and his wife were seized in the raid. Federal agents returned the equipment after determining that no one at the home had downloaded the illegal material. Agents eventually traced the downloads to a neighbor who had used multiple IP subscribers' Wi-Fi connections (including a secure connection from the State University of New York). See Carolyn Thompson, *Bizarre Pornography Raid Underscores Wi-Fi Privacy Risks* (April 25, 2011), www.msnbc.msn.com/id/42740201/ns/technology_and_science-wireless/

32. Plaintiff was or should have been aware of the facts outlined in paragraph 31 at the time it filed the action against the Doe defendants, including Defendant, in this case on February 15, 2012.
33. Furthermore, the plaintiff makes these statements in the Complaint even though it knew or should have known that even if a computer was used to illegally download, copy, and distribute its materials through the IP addresses it identifies in the Complaint, that fact in no way ties the act to the subscriber. The act could have been done by another person with a computer connected to the IP address without the knowledge or consent of the subscriber. In the case of a wireless internet connection, the alleged infringing activity could have been performed by any person with a computer within range of the wireless network, a fact of which the plaintiff was or should have been well aware. It could also have been done from a remote location by an individual or entity who had “spoofed” or duplicated the subscriber’s IP address, a fact of which the plaintiff was or should have been well aware. Plaintiff was or should have been aware of all of these facts at the time it filed the action against the Doe defendants, including Defendant, in this case on February 15, 2012.
34. The high error rate of the IP “harvesters” has been acknowledged by at least one pornography company plaintiff. In one case in the Southern District of New York, counsel for the plaintiff “estimated that 30% of the names turned over by ISPs are not those of individuals who actually downloaded or shared copyrighted material.” Opinion and Order, *Digital Sin, Inc. v. John Does 1-176*, 2012 W.L. 263491, 12-cv-00126 (S.D.N.Y. Jan. 30, 2012), at p. 5. This high error rate, shocking in and of itself, is compounded by the nature of the allegations that the Complaint makes public – namely, the illegal download of hardcore pornographic materials – which can have a devastating effect on the personal and professional lives of those falsely accused.

35. Upon information and belief, Plaintiff knows that it has at least a similar error rate if not higher. As such, Plaintiff knows with a certainty that as a matter of fact it is pursuing hundreds of innocent individuals. This is especially important when coupled with Plaintiff's continued refusals to accept proffers of evidence from those who have been innocently accused, instead choosing to pursue their extortion business model against innocent people with total disregard for the damage done to the lives of those wrongfully accused.
36. To highlight the recklessness and malice with which Plaintiff in this case has acted, if for example a federal prosecutor were to bring criminal charges of, say, downloading child pornography based upon harvested IP addresses with a known error rate of approximately 30%, not only would that be a clear abuse of process – not to mention running afoul of numerous Constitutional protections – but would likely be criminally actionable prosecutorial misconduct. By the same token, no civil attorney would bring such frivolous and misguided lawsuits – the cost of which would bankrupt the average plaintiff – based on a known 30% rate of innocence without seriously implicating duties under Federal Rule of Civil Procedure 11 as well as 28 U.S.C. 1927. Such actions as those demonstrated by this Plaintiff and its attorney personify a policy of “shoot first, ask questions later” style of litigation.
37. The plaintiff company next files a motion requesting expedited discovery, seeking leave to serve subpoenas upon the ISPs (Internet Service Providers) that issued the IP addresses. (In this case, Plaintiff filed its Motion for Leave to Serve Third Party Subpoenas Prior to a Rule 26(f) Conference on February 16, 2012, only one day after filing the Complaint. Defendant, of course, was never served with this motion and had no opportunity to oppose it because at that point, everyone, including the Court, was unaware of Defendant's identity.)

38. The subpoena commands the ISP to release personal identifying information of the subscriber associated with that IP address – generally, the individual's name and address; often, his or her telephone number and email address as well. Because the Does are unknown and never find out about it, the motion stands unopposed. Throughout the Motion papers, Plaintiff repeatedly insisted that by finding out the identity of the owner of the IP address, Plaintiff would identify the infringer: "Since Defendants used the Internet to commit their infringement, Plaintiff only knows Defendants by their Internet Protocol ("IP") addresses." (Motion, p. 1); "Defendants are all copyright infringers..." (Motion, p. 6). These statements are entirely misleading, as described in detail above, but as the motion was unopposed, there was no one to point out the Plaintiff's fallacious conclusions to the court. In reliance on the unfounded and false representations of the plaintiff company and its counsel – which the Doe defendants have no opportunity to oppose – the court grants leave for plaintiff to issue the subpoenas. In *Malibu Media v. John Does 1-30*, the court entered an Order Granting Leave to Serve Third Party Subpoenas Prior to a Rule 26(f) Conference on February 21, 2012.

39. The plaintiff knows and intends that the ISPs will pass along the subpoenas to the subscribers whose identifying information is sought. A Doe defendant faced with such a subpoena is unlikely to be sophisticated or knowledgeable about the law, and is likely to be frightened and intimidated by the receipt of such a document. In most cases, a Doe defendant will be unaware of his or her right to move the court to quash the subpoena or to ask to proceed anonymously; even if the Doe defendant knows of this right, in many cases, he or she is unlikely to be able to afford an attorney to do so. The Doe defendant, afraid of being involved publicly in such an unseemly litigation – indeed, in any litigation – may simply contact the plaintiff's counsel in an attempt to make the problem go away. Or, the Doe defendant may simply ignore the

notice, which will result in the ISP's turning over of his or her personal identifying information to the plaintiff.

40. Once the plaintiff is in possession of the personal identifying information of the Doe defendants, the plaintiff begins a process of trying to coerce settlements. Depending on the plaintiff's business plan, this may begin with high-pressure phone calls or letters, but it always involves informing the defendant that he or she is about to become the target of a litigation that will accuse him or her of downloading pornography; that the defendant stands to lose hundreds of thousands of dollars in statutory damages and attorney's fees for each alleged incident, not to mention having to retain an attorney on his or her own behalf; and that the defendant can make it all go away for a comparatively small amount of money, usually several thousand dollars. See **Exhibit F**, settlement letter sent to LiuXia Wong, filed in *LiuXia Wong v. Hard Drive Productions, Inc., and Does 1-50*, 4:12-cv-00469. In no instance is any offer of innocence, or even an offer to inspect a John Doe's personal computer, accepted. Such a personalized investigation would simply be too time consuming and would hurt the business model by actually discovering that many of those who stand accused are in fact innocent.

41. Upon information and belief, it is in fact Plaintiff's as well as opposing counsel's express purpose to remain willfully ignorant of potential defenses as well as errors in IP collection techniques. Indeed, Plaintiff and Plaintiff's counsel have already been directly warned by one Court that similar litigation behavior was inappropriate, abusive and unfair. See, *In Re BitTorrent Adult Film Copyright Infringement Cases*, 2012 U.S. Dist. LEXIS 61447 at *19 (E.D.N.Y. 2012). In that case, the Court admonished Plaintiff and attorney Kotzker that it had "employed abusive litigation tactics to extract settlements from John Doe defendants"). Indeed, the Court went so far as to describe Plaintiff's justifications for such tactics as "rambling" and "farcical."

Id. at n7. More on point, the Court even identified Plaintiff's desire to remain willfully ignorant of potential defenses merely to maintain their for-profit business model and pressure potential John Does out of thousands of dollars. In particular, the Court noted that at least one Defendant offered Plaintiff and its attorney Mr. Kotzker "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."

42. Upon information and belief, similar offers of proof have been made to Plaintiff and its counsel Mr. Kotzker which have been summarily refused. Such abusive tactics demonstrate a lack of good faith and willful disregard of all Rule 11 duties to conduct a reasonable pre-filing inquiry into the evidentiary and factual support for a litigant's claims. They also represent an abuse of process, and as this Court has noted makes defendants' lives and reputations mere "cogs in plaintiff's copyright-enforcement business model." *Malibu Media, LLC v. Felitti*, 2012 U.S. Dist. LEXIS 103393 at *14 (D. Colo. 2012).
43. Upon information and belief Plaintiff and its counsel would have refused any offer of proof from Defendant.
44. In addition, upon information and belief, part of Plaintiff's business model is to stonewall all legitimate discovery requests and make blanket assertions of confidentiality and/or privilege to prevent anyone from discovering the Plaintiff's real motivations and litigation techniques. These are further abuses of the judicial process.
45. If the plaintiff companies truly were concerned about protecting their copyrights and preserving the profits thereon, one would expect to see such companies take certain actions once they had the IP addresses and personal information obtained through their investigations and lawsuits. One would expect to see plaintiff companies

issuing Digital Millenium Copyright Act (DMCA) takedown notices, or sending out cease-and-desist letters, or seeking injunctive relief in the courts. Such a course of action would be reasonable to expect in a company that sought to minimize illegal downloads, mitigate damages, and protect its copyrights. However, that is not the course of action pursued by these pornography companies. To the contrary, not only do they not remove their films from the internet, they encourage the continued downloading of their works through the use of “honeypots” in order to promote the income stream to be obtained through settlements of threatened lawsuits.

46. In this regard, upon information and belief, Plaintiff does not operate a business to create, market and sell its alleged pornographic films, but instead has created a shell business solely for the purposes of uploading its own works out on BitTorrent platforms to encourage and promote infringement of its works, and then sit back and generate revenue from high pressure and abusive litigation tactics against the very people it encouraged and entrapped. Such actions smack of champerty and barratry and represent an abuse of process.

47. Due to the vast number of individuals being sued, the burden of pursuing these Does is passed on to a “call center” where non-attorney agents acting on behalf of the plaintiff repeatedly call, harass and threaten the Does, who often have no idea that their information was even turned over to the plaintiff by their ISP. The “call center” employees refuse to provide any type of contact information such as a return phone number or email address, and they refuse to provide information about who they actually work for. These calls can go on for months. They often contain threats of criminal prosecution for “exposing minors to pornography” and pointedly remind the Doe defendant that they do not want the publicity that a lawsuit would bring. One Colorado Doe defendant was threatened with such criminal action in exactly this way, and was told ominously that he wouldn’t want to see his name in the Denver

Post. See, **Exhibit G**, Declaration of John Doe, ¶¶ 5 and 3. This Doe was also threatened that the company that gathered the information on his IP address could tell whether he had sold the allegedly downloaded movie and whether he had downloaded other copyrighted material in which case, they would sue him for that too. Exhibit G, ¶ 6. He was also told explicitly that if he did not settle, they would sue. These harassing phone calls continued, with only a short break, for a period of fourteen months. Exhibit G, ¶10.

48. Based upon information and belief, counsel for Plaintiff does not even engage in settlement discussions with putative defendants in this or other Plaintiff's other similar BitTorrent cases. Defendant has never been contacted by Mr. Kotzker for the purpose of settlement discussions, but instead, he has received calls from one Anthony Palmer a "representative" of Plaintiff. Upon information and belief, the "call center" is being actively used by Plaintiff and Plaintiff's counsel in this case and numerous other Colorado BitTorrent cases referred to in this document to make continuing harassing and intimidating phone calls to Doe defendants, threatening them with public humiliation and, in some cases, with criminal action. The sole purpose of these threats and statements is to coerce the Doe defendants into paying a quick monetary settlement of a few thousand dollars without Plaintiff and Plaintiff's attorney having to file an additional lawsuit (after the Doe lawsuit in which the defendant's identifying information was obtained). Upon information and belief, the "call center" acts as Plaintiff's agent in this matter and these threats and intimidating statements are made with the full knowledge of Plaintiff and Plaintiff's counsel, and in fact at the direction of Plaintiff and/or Plaintiff's counsel and/or some other individual acting on Plaintiff's behalf.

49. Upon information and belief, numerous John Does who are represented by counsel have nevertheless been contacted by these “call centers” in contravention of the Colorado Rules of Professional Conduct.
50. The plaintiff pornography companies utilize the emotional impact of their lawsuits, or threat thereof, in order to manipulate, influence and coerce the Doe defendants into settling. There can be no doubt that it is a frightening prospect to be part of a lawsuit, to say nothing of the prospect of thousands or hundreds of thousands of dollars in attorney’s fees, which most people – Defendant included – cannot afford. Moreover, these pornography companies rely upon the public stigma which attaches to the accusation of having downloaded pornography and the scorn and disgust which such an idea engenders in the public mind. That this distasteful act was also committed illegally increases the harm of the accusation exponentially. Separate or combined, these accusations, if made public, may brand and stigmatize the innocent accused in ways that may be difficult if not impossible to overcome. Family relationships, friendships, community standing, business and commercial opportunities, career advancement, eligibility to run for or assume public office, the ability to work in any capacity with children or youth groups in ways such as teaching, coaching, or scouting volunteer, the ability to gain security clearance, eligibility for the Bar or medical school admission, qualification for a passport or visa: all of these may be adversely impacted by the allegation, even if it is never proven. Such allegations, knowingly based on grossly inaccurate information, is the quintessential definition of a willful abuse of the judicial process that has a devastating effect on the wrongly accused.
51. In this manner, these pornography companies can sue thousands of Doe defendants and, based upon APMC’s estimates, they can expect a 35% settlement rate with payoffs from hundreds of Does in thousands of dollars. A truly terrified Doe

defendant – one who, like a teacher, stood to lose their livelihood – might settle for tens of thousands of dollars. Thus, with very little effort on its part, a pornography company could profit substantially by simply collecting information about individuals who are engaging in any kind of activity on the internet.

52. This “for-profit litigation model” is especially pronounced as the Court begins to appreciate the sheer magnitude of the numbers of potential John Does that can be named in a single or even multiple lawsuits by a single attorney. As here, it would be impossible for the pornography company plaintiffs to actually litigate against every IP addresses harvested. In that sense, the only way that such a model can work is to assert weak claims of copyright infringement, while evading any type of judicial review of the merits of the actual case. As time passes and courts begin to question why such cases never progress, the plaintiffs then file a few token suits against individuals to provide a patina of legitimacy, as was done in the instant case against Defendant, Mr. Deus and Mr. Dunn.

53. Upon information and belief, such individual lawsuits were only filed based on an Order to Show Cause issued to Plaintiff by the Court as to why the various BitTorrent cases, all of which are handled by Plaintiff’s counsel Kotzker, were not being prosecuted. In addition, upon information and belief, additional lawsuits against named individuals were entered only after Plaintiff was countersued in this action and were done for the sole purpose of insulating Plaintiff and its counsel from claims of abuse of process.

54. Upon information and belief, Plaintiff has filed several hundred lawsuits across the country, but has not named or served any persons outside of Colorado where it has been aggressively countersued. Such an insulating tactic represents an abuse of process where such suits were not brought based on the merits of the cases but

merely to avoid potential liability and to provide the patina of legitimacy to Plaintiff's abusive for-profit litigation campaign.

55. Upon information and belief, Plaintiff has not yet filed individual lawsuits against hundreds if not thousands of individuals whom it has accused as Doe defendants in order to obtain their personal identifying information. Defendant further believes and is informed that Plaintiff has no plan or desire to name and sue these individuals.

56. Upon information and belief, Plaintiff is merely an undercapitalized litigation vehicle with no real substantial assets and no insurance. Upon information and belief, Plaintiff could not financially pursue litigation against even a fraction of the Doe defendants that it accuses due to the exposure risk of fee-shifting provisions of the Copyright Act. Such facts further demonstrate Plaintiff's true motives and abuse of the judicial process.

57. As the Fifth Circuit recently affirmed in *dicta*, not surprisingly in affirming contempt sanctions for an identical "copyright troll" "[t]his course of conduct indicates that the plaintiffs have used the offices of the Court as an inexpensive means to gain the Doe defendants' personal information and coerce payment from them. The plaintiffs seemingly have no interest in actually litigating the cases, but rather simply have used the Court and its subpoena powers to obtain sufficient information to shake down the John Does. Whenever the suggestion of a ruling on the merits of the claims appears on the horizon, the plaintiffs drop the John Doe threatening to litigate the matter in order to avoid the actual cost of litigation and an actual decision on the merits." *Mick Haig Production v. John Does 1-670, v Evan Stone; Order affirming contempt sanction, Case 11-cv-10977, pg, 6, July 12, 2012; citing Raw Films, Ltd. v. Does 1-32, 2011 WL 6182025, at *3 (E.D. Va. 2011)*

58. That this is a nationwide campaign akin to a plague of locusts cannot be denied. What started in or about 2010 had by January of 2011 impacted some 100,000

individuals in the United States. <https://torrentfreak.com/100000-p2p-users-sued-in-us-mass-lawsuits-110130/>. By August of 2011, that number had passed the 200,000 mark <http://torrentfreak.com/200000-bittorrent-users-sued-in-the-united-states-110808/>, and by February, 2012, the number had passed 250,000. Tens of thousands of individuals every month are being victimized by this extortionate scheme. A review of various Court's dockets show that such huge numbers are being pursued by only a handful of attorneys around the country, perhaps fewer than twenty. As such, it is clear to any reasonable observer that such suits are essential to mass "for-profit" litigation schemes that are not designed to be actually litigated in court, but merely enforced through harassing phone calls and threatening letters, with the occasional "token" suit being filed to intimidate and frighten the others into wondering: "Will I be next?"

59. Upon information and belief, none of these hundreds of thousands of cases has ever reached a jury, or even had any meaningful discovery.
60. Upon information and belief, the mastermind and driving force behind many of the copyright trolls, including Malibu Media, LLC, is a Florida attorney named M. Keith Lipscomb, Esq. Mr. Lipscomb represents Malibu Media, LLC, in its Florida cases; see, e.g., 3:12-cv-00336.¹³ In an email, Mr. Lipscomb asserts to Brad Patrick, Esq., an attorney representing several Doe defendants, that Mr. Lipscomb's clients include Patrick Collins, Inc. and K-beech, Inc., and that "my clients' lawyers" will begin filing suits for copyright infringement in a multitude of jurisdictions: that as of the date of the email, July 1, 2011, they had already filed "over 50 federal cases in NY, CA, DC, MD, VA, NY, NJ, CO, FL and my clients have counsel in and new cases will soon be filed in NC, OH, PA. Further we have counsel retained and any moment cases in TX,

¹³ In a Declaration submitted to the court in this case in Florida, Mr. Lipscomb asserted that he expected settlements from about half of the Doe defendants once he obtained their identifying information from the ISPs.

AZ, IL, CT, GA. (sic)" **Exhibit H**, email dated July 1, 2011, p. 1. This clearly evinces a nationwide strategy with several layers of attorneys and clients involved. The current flooded state of the Federal docket shows that Mr. Lipscomb's plan is being implemented.

61. Upon information and belief, Plaintiff's Colorado counsel was recruited by Mr. Lipscomb to be part of his "network" with the promise of significant contingency fees based on settlements wrested from Doe defendants. Upon further information and belief, Mr. Kotzker is actually under the direction of Mr. Lipscomb, not the Plaintiff.
62. Upon information and belief, Mr. Lipscomb, Mr. Kotzker and Malibu Media LLC have entered into a champertous and barratrous relationship
63. Mr. Lipscomb's plan is, in his own words, "a campaign." Exhibit H, p. 2. Mr. Lipscomb warns Mr. Patrick that his motions to quash filed on behalf of his Doe defendant clients were "impeding our ability to use the court system..." and that "[w]e cannot stand for that under any circumstances. Accordingly, the state court arguments have been teed up and to exert the maximum amount of pressure that we can we are filing (sic) to file individual federal suits *to teach your clients the lesson that this is not the way to deal with us.*" Id. (emphasis added). Mr. Lipscomb, the mastermind of the pornography companies' legal strategy, is quite clear: when Doe defendants resist, it will not be tolerated and those Does must be taught a lesson, and the means of imposing that lesson is the filing of a federal lawsuit.
64. Moreover, Mr. Lipscomb reveals that the filing of such federal suits will not be burdensome or difficult for these attorneys because "the federal court suits have been standardized." Id. Thus, for all of the clients Mr. Lipscomb represents and/or advises – and upon information and belief, this includes the Plaintiff – there is very little cost or effort required to file and prosecute the federal lawsuits, as the work has already been prepared and "standardized."

65. Mr. Lipscomb warns Mr. Patrick not to “test” him. “[I]f we have to file suit, our settlement demands will increase. Toward that end, you should also apprise your clients that the average cost of a copyright litigation is 600K through trial, according to an AIPLA survey of fees in IP cases.” Exhibit H, p. 2.

66. One month later, in a subsequent email, Mr. Lipscomb threatens Mr. Patrick’s clients with further litigation if they do not settle:

...you can tell your clients that IPP¹⁴ is one of three companies doing these scans and that they have provided me with information which establishes several of your clients infringed movies from studios that I do not represent. In my individual suits, I am going to call all of those studios and have them become additional plaintiffs. Right now, statistically there is only about a .1 percent chance they’ll get hit by these studios with a suit. Then I am going to go the (sic) other two companies that scan and get all the other plaintiffs I can from all of them.

Exhibit I, email dated August 25, 2011.

67. Mr. Lipscomb is the attorney involved in the case of the Colorado Doe defendant who has been repeatedly harassed by telephone calls from a call center in Florida. One Mr. Stern, calling on behalf of Mr. Lipscomb’s law firm, informed the Doe defendant that he was involved in a lawsuit in a Florida court. Mr. Stern, on Mr. Lipscomb’s behalf, also told Doe, among other threats, that because he maintained an open wireless connection, he was facing criminal prosecution for exposing minors to pornography. Further, Mr. Lipscomb himself sent Doe a letter informing him that if he did not settle, Lipscomb would sue. Exhibit G.

68. Upon information and belief, counsel for Plaintiff, Mr. Kotzker, is directly associated with, and indeed takes direct instructions from, Mr. Lipscomb and that the two are

¹⁴ IPP is the same “harvesting” company retained by Plaintiff herein, yet another indication of the connection between Mr. Lipscomb and Plaintiff. If IPP’s collection techniques mistakenly obtained Defendant’s IP address, it is not unlikely that IPP collection techniques also mistakenly obtained the information asserted here by Mr. Lipscomb, nor is it unlikely that Mr. Lipscomb was well aware of that fact.

jointly involved in Plaintiff's nationwide "campaign." Upon information and belief, Mr. Lipscomb specifically instructed Mr. Kotzker to file against a Doe defendant in Colorado because Mr. Patrick would not withdraw his motions to quash; this is alluded to in Mr. Lipscomb's email of July 1, 2011: "So, if they want to test me sooner, just pick a Doe in Florida, Colorado or California and say he is not going to settle today and that suit will be filed over the weekend." Exhibit H, page 2.

69. Upon information and belief, attorney Kotzker, under the direction of Mr. Lipscomb, then filed suit against a Doe defendant in Colorado as a direct retaliation for other defendants' – who were represented by a different attorney – exercising their right to file motions to quash the subpoenas that sought their personal information, just as Mr. Lipscomb's email threatened would occur. Such retaliatory litigation was brought for an improper purpose and is an abuse of process.

The Plaintiff's Actions Leading Up To The Current Litigation

70. Upon information and belief, Plaintiff utilized a "honeypot" to lure potential infringers. Plaintiff admits as much by grounding its Complaint upon an alleged download by all of the defendants herein of "most of a website containing 107 movies." Complaint ¶2. The fact that there were 107 films together in one digital file, thirteen of which were allegedly owned by Plaintiff (Complaint ¶¶ 3, 15), is indicative of a "honeypot." Upon information and belief, Plaintiff and/or its employees and/or IPP Ltd., acting as its agent and with its authorization and consent, intentionally placed these films together and created a "honeypot."

71. Plaintiff utilized IPP Ltd., a third party investigator, to "harvest" information regarding IP addresses. Complaint ¶40. Upon information and belief, as part of the process of "harvesting" IP addresses, companies such as IPP Ltd., must upload an original copy of the digital file in order to participate in a "swarm" and track downloads and obtain

IP addresses allegedly involved in BitTorrents. Thus, Defendant is informed and believes that Plaintiff either created and uploaded the website of 107 movies which it claims the three defendants in this action infringed, or it authorized IPP Ltd., to do so with the specific purpose of tracking IP addresses and initiating lawsuits.¹⁵

72. Having collected IP addresses through IPP Ltd., Plaintiff has followed the “copyright troll” business model and has filed hundreds of “John Doe” lawsuits against thousands of Doe defendants in fourteen separate Federal district courts. As of the filing of the original Answer and Counterclaim, Plaintiff had brought cases in California, Colorado, the District of Columbia, Florida, Maryland, New York, Pennsylvania and Virginia. In the short time since then, Plaintiff has expanded into Illinois, Indiana, Kentucky, Michigan, New Jersey and Texas. See, <http://dockets.justia.com/search?query=malibu+media>. This is in line with the nationwide “campaign” delineated in Mr. Lipscomb’s letter.

73. Now in possession of personal information of hundreds of Colorado Doe defendants and thousands of Does in other states, Plaintiff has not behaved in a manner to protect its copyrights and mitigate its damages. Upon information and belief, it has not caused any Digital Millennium Copyright Act (DMCA) takedown notices to be issued, it has not sent any cease-and-desist letters, and it has not sought injunctive relief or any restraining orders against the Does against the use or distribution of Plaintiff’s allegedly copyrighted films.

74. Because Plaintiff has consistently been criticized for its failure to prosecute its cases against the hundreds of Does it has sued to obtain personal information, it has commenced a sudden flurry of suits against individual Colorado defendants, filing multiple cases against named Does. This was undoubtedly prompted by a show

¹⁵ As noted above, Defendant denies having participated in any BitTorrent that may have downloaded any of Plaintiff’s allegedly copyrighted films. There are many different ways that IPP Ltd. may have erroneously or falsely obtained the IP address assigned to Defendant’s account by Qwest/CenturyLink.

cause order issued to Plaintiff's counsel, Mr. Kotzker, for lack of prosecution of Plaintiff's numerous cases, and by Judge Martinez' order of July 25, 2012, severing and dismissing Plaintiff's case against six named defendants (Malibu Media LLC v. Felitti et al, 1:12-cv-1522-WJM). See, <http://dockets.justia.com/search?query=+malibu+media&state=colorado>, which shows eleven cases filed on July 11, 2012, against named defendants; as well as four more cases against 111 Doe defendants.

The Case Before This Court

75. Plaintiff commenced the instant action against the Defendant by filing a suit against thirty "John Does" (Case No. 1:12-cv-00402) on or about February 15, 2012. The sole purpose of that action was to obtain the issuance of subpoenas to the John Does' internet service providers (ISPs) in order to determine the identity of the John Does.

76. On or about February 15, 2012, Plaintiff also filed seven other cases as follows:

Malibu Media LLC v. John Does 1-29	Case No. 1:12-cv-00397
Malibu Media LLC v. John Does 1-27	Case No. 1:12-cv-00406
Malibu Media LLC v. John Does 1-27	Case No. 1:12-cv-00409
Malibu Media LLC v. John Does 1-18	Case No. 1:12-cv-00407
Malibu Media LLC v. John Does 1-16	Case No. 1:12-cv-00399
Malibu Media LLC v. John Does 1-15	Case No. 1:12-cv-00408
Malibu Media LLC v. John Does 1-10	Case No. 1:12-cv-00405

77. On or about April 2, 2012, Plaintiff filed two more such cases, as follows:

Malibu Media LLC v. John Does 1-28	Case No. 1:12-cv-00834
------------------------------------	------------------------

Malibu Media LLC v. John Does 1-21	Case No. 1:12-cv-00835
------------------------------------	------------------------

78. On or about April 3, 2012, Plaintiff filed seven further such cases, as follows:

Malibu Media LLC v. John Does 1-9	Case No. 1:12-cv-00846
Malibu Media LLC v. John Does 1-23	Case No. 1:12-cv-00836
Malibu Media LLC v. John Does 1-17	Case No. 1:12-cv-00839
Malibu Media LLC v. John Does 1-16	Case No. 1:12-cv-00840
Malibu Media LLC v. John Does 1-11	Case No. 1:12-cv-00843
Malibu Media LLC v. John Does 1-10	Case No. 1:12-cv-00837
Malibu Media LLC v. John Does 1-6	Case No. 1:12-cv-00845

79. On or about April 4, 2012, on the same day that Plaintiff filed the current action against Defendant and the other defendants, Plaintiff filed an additional case against one more John Doe as Case No. 1:12-cv-00885.

80. On or about May 29, 2012, Plaintiff filed a case against one John Doe as Case No. 1:12-cv-01386.

81. On or about May 30, 2012, Plaintiff filed eight more cases, as follows:

Malibu Media LLC v. John Does 1-14	Case No. 1:12-cv-01406
Malibu Media LLC v. John Does 1-15	Case No. 1:12-cv-01408
Malibu Media LLC v. John Does 1-33	Case No. 1:12-cv-01394
Malibu Media LLC v. John Does 1-5	Case No. 1:12-cv-01395
Malibu Media LLC v. John Does 1-5	Case No. 1:12-cv-01404
Malibu Media LLC v. John Does 1-5	Case No. 1:12-cv-01405

Malibu Media LLC v. John Does 1-54	Case No. 1:12-cv-01407
------------------------------------	------------------------

82. On or about June 12, 2012, Plaintiff filed an action against six named defendants, 1:12-cv-1522. There is no way of knowing which of the hundreds of Does these defendants are. On July 25, 2012, Judge Martinez entered an Order which found joinder of these defendants improper and dismissed the cases against all but one of the defendants without prejudice. To date, Plaintiff has not refiled against those other defendants.

83. On or about June 27, 2012, Plaintiff filed yet another action against 19 Does, as Case No. 1:12-cv-1692.

84. On or about July 18, 2012, Plaintiff filed against eleven individual defendants, as Case Nos. 1:12-cv-1866 through 1:12-cv-1876.

85. On or about July 27, 2012, Plaintiff filed yet another action against 42 Does, as Case No. 1:12-cv-.1953.

86. On or about August 6, 2012, Plaintiff filed three more cases, as follows:

Malibu Media LLC v. John Does 1-14	Case No. 1:12-cv-02071
Malibu Media LLC v. John Does 1-24	Case No. 1:12-cv-02070
Malibu Media LLC v. John Does 1-31	Case No. 1:12-cv-02069

87. The attorney representing plaintiff here in Colorado and who has filed these 30-plus cases is the same attorney who filed twenty-five separate cases against hundreds of John Does in the Federal District Courts for the Southern and Eastern Districts of New York on behalf of Malibu Media LLC. This same attorney, representing Patrick Collins, Inc., has filed more than thirty-seven copyright infringement cases against

Doe defendants in New York, and over nineteen such cases in Colorado. Malibu Media LLC, Patrick Collins, Inc., and Third Degree Films, Inc., expanded into New Jersey last month, filing fifteen cases against nearly five hundred people between them. See,

[http://www.northjersey.com/news/business/tech_news/Thousands in NJ are targeted by file-sharing lawsuits.html?page=all](http://www.northjersey.com/news/business/tech_news/Thousands_in_NJ_are_targeted_by_file-sharing_lawsuits.html?page=all). Upon information and belief, Plaintiff's attorney, Jason A. Kotzker, does not maintain a physical office in Colorado, but instead uses a Post Office Box as his only address within the state. See, ABC 7 local television news report, <http://www.thedenverchannel.com/news/31030100/detail.html>. The sheer number of cases filed by Plaintiff and handled by Mr. Kotzker begs the question: how can one attorney diligently prosecute hundreds of cases at the same time in jurisdictions which are some two thousand miles apart? The answer, of course, is that neither he nor Plaintiff have any expectation that he will have to, because they anticipate settlements from the majority of the Doe defendants before they ever have to start moving forward into litigation. The entire business model is built on this premise, and the results they have achieved (as enumerated herein) bear it out.

88. Upon information and belief, Plaintiff and its counsel knew or should have known this prior to initiating every single action. Such filings being made with a sure knowledge that one cannot possibly and/or will not prosecute each and every suit should that be necessary, is an abuse of process and a violation of the Rules of Professional Conduct, R. 1.3.

89. On or about February 22, 2012, a subpoena was issued in the case of *Malibu Media LLC v. John Does 1-30*, Case No. 1:12-cv-00402 to Qwest/CenturyLink seeking the personal identifying information of Defendant and eight other Doe defendants (Does

Number 22-30). Qwest/Century Link provided a copy of this subpoena to Defendant. See **Exhibit J**, letter and subpoena.

90. In that letter from Qwest/CenturyLink, Defendant was informed that he had until March 15, 2012, to notify Qwest/CenturyLink in writing of any objections and further, that it was necessary to “file your objections with the court on or before the date specified to prevent the release of your records pursuant to the subpoena.” Id.

91. This placed Defendant in the position of either attempting to quash the subpoena on his own behalf, in which case he would have to appear in court *pro se* and thereby provide to Plaintiff exactly the information it sought to obtain by the subpoena, or having to hire an attorney to bring a motion to quash on his behalf, which would have required a great deal of expense and could potentially have also resulted in Defendant’s personal identifying information being provided to the Plaintiff if the court did not permit Defendant to proceed anonymously (not all courts have done so). Moreover, at that point, Defendant did not comprehend the nationwide scope and malicious intent of the Plaintiff and the other copyright trolls. Defendant did not attempt to quash the subpoena.

92. On or about March 22, 2012, a person named Anthony Palmer telephoned Defendant. He represented to Defendant that he was calling on behalf of Malibu Media and told Defendant that he was the “primary” and/or “main” defendant in a lawsuit about to be filed. He urged Defendant to obtain an attorney and to settle the matter. Upon information and belief, Mr. Palmer works for the aforementioned “call center” overseen by Mr. Lipscomb and Mr. Kotzker.

93. Defendant did not settle because he is innocent.

94. On or about April 4, 2012, the instant case was filed against these defendants.

95. By April 5, 2012, the first of the Doe defendants were starting to settle. An examination of the court's P.A.C.E.R. website reveals the following regarding the other Doe defendants Malibu Media sued along with Defendant:

DATE	AS TO DOE DEFENDANTS	DISPOSITION
4/5/12	8,23,24,25,29	Dismissed w/out prejudice
4/5/12	9,17,20	Settled and dismissed w/ prejudice
4/10/12	4	Settled and dismissed w/ prejudice
4/17/12	22	Settled and dismissed w/ prejudice
4/30/12	2,12,13,21,26,27,30	Dismissed w/out prejudice
4/30/12	1	Settled and dismissed w/ prejudice
5/30/12	3	Settled and dismissed w/ prejudice
6/14/12	6,7,10,11,14,15,16,19,28	Dismissed w/out prejudice because Plaintiff's attorney stated he would be unable to serve these defendants within the time required by the rules of court
7/5/12	18	Settled and dismissed w/ prejudice

96. Thus, out of the thirty defendants sued by Plaintiff on February 15, 2012, eight settled before they were even named in a lawsuit. Presumably three of these Does are the three defendants named in the current action, although there is no way to be certain of that since Plaintiff and its counsel are in sole possession of the Does' identifying information. Significantly, Plaintiff is still in possession of the personal identifying information of nineteen individuals who face the prospect of a lawsuit being brought against them if they do not settle.

97. On or about April 6, 2012, and April 9, 2012, Defendant received voice mail messages from Plaintiff's agent Anthony Palmer again stressing that he was the "main" defendant in a lawsuit and advising him to get an attorney and contact him regarding settlement. Mr. Palmer told Defendant to "Google" his name so he could see that the case had been filed. Defendant did not return these phone calls.

98. On or about May 5, 2012, Defendant was served with the Complaint in the instant matter. Service was made at Defendant's home on a Saturday morning when his

family and neighbors were at home. His eleven-year-old son answered the door and told Defendant the police had arrived.

99. The communications from Plaintiff's agent Anthony Palmer and the manner in which the Defendant was served were clearly designed and intended to embarrass, manipulate and intimidate Defendant and coerce him into settling despite his innocence and despite the absence of any evidence against him.

COUNT I

ABUSE OF PROCESS

100. Defendant restates and realleges all of the allegations of the previous paragraphs as if more fully stated herein.
101. Plaintiff has wrongfully, improperly and illegally used the Federal Court system in an effort to obtain money from this Defendant, the other two defendants in this matter, and the multitude of other defendants which Plaintiff has sued in nine other Federal District Courts.
102. The filing of the initial case, *Malibu Media LLC v. John Does 1-30*, Case No. 1:12-cv-00402-WYD, was done solely with the intent of generating the subpoenas which would provide the identifying information of the individual defendants and to no other purpose. Plaintiff's case was devoid of factual support and without cognizable basis in law. The Declaration of Tobias Fieser upon which that Complaint relied is tainted by financial interest and is factually flawed.
103. At the time that the initial case was filed, Plaintiff had no knowledge as to the identities of any of the Doe defendants, and therefore, Plaintiff could not honestly represent to the court that the Doe defendants were the infringers. For all of the reasons listed above in paragraphs 24-27 and 31, there was no information

indicating that Defendant – or any of the Doe defendants, for that matter – was the individual who infringed Plaintiff’s alleged copyrights, if indeed there ever was any infringement at all. Plaintiff knew this at the time that the Doe complaint was filed in this matter and yet represented to the court as *fact* that the Doe defendants were guilty of infringement. This was a knowing misrepresentation then, as it is now.

104. At the time that the initial case was filed, Plaintiff had no knowledge as to the identities of any of the Doe defendants, and therefore, Plaintiff could not honestly represent to the court that any reason to join all of these individuals existed. According to the information provided by Plaintiff to the court, the individual acts were alleged to have taken place on separate, distinct dates and times (see Exhibit J) and were in no way connected, and therefore, each individual John Doe ought to have been sued separately and each subpoena issued separately. By filing the case against multiple defendants in this way, Plaintiff evaded over ten thousand dollars in filing fees which ought to have lawfully been paid to the Court.

105. In substantially similar cases filed by Plaintiff and Plaintiff’s attorney in New York state, Plaintiff and Plaintiff’s attorney have been repeatedly taken to task and threatened with sanctions for their misconduct with regard to the privacy of the Doe defendants. In *Malibu Media v. John Does 1-5*, 2012 WL 2001968 (S.D.N.Y. June 1, 2012), Plaintiff and its attorney Kotzker were denied access to Doe defendants’ telephone numbers specifically so that they could not engage in harassing phone calls to the Doe defendants. Currently, Plaintiff and its attorney Kotzker are awaiting the result of a show cause order, also in New York, why attorney Kotzker should not be sanctioned for failure to comply with the specific terms of a May 1, 2012, court order requiring the responses to Plaintiff’s subpoenas to ISPs to be produced directly to the court *ex parte* and under seal. The subpoenas went out of attorney Kotzker’s office to the ISPs directing them to produce the information regarding the identifying

information of the Doe defendants directly to attorney Kotzker. *In re BitTorrent Adult Film Copyright Infringement Cases*, 2:11-cv-03995 (E.D.N.Y.).

106. In addition, upon information and belief, Plaintiff has failed to comply with court rules in other jurisdictions. In the Central District of California, as of June 27, 2012, Plaintiff had filed 28 Doe defendant cases and had not filed a single Notice of Related Cases as required by Local Rule 4.3.

107. In addition, upon information and belief, Plaintiff has engaged in forum shopping by filing cases that involve defendants that do not live in the jurisdiction in which the case is filed and judge shopping by filing multiple cases in one jurisdiction so that each case will be assigned to a different judge in the hope of getting a judge whose outlook will be more favorable to Plaintiff's side of the matter. See, e.g., 3:12-cv-00335 and 3:12-cv-00336, (in which Plaintiff's counsel, Lipscomb, was ordered to explain why these cases were filed separately)

108. In this case, Plaintiff made misleading, false and fraudulent statements to the Court in order to convince the Court to grant its motion to issue subpoenas. Further, Plaintiff intentionally and maliciously misused the information obtained from those subpoenas to effect an object not within the proper scope of the subpoenas: namely, the extortion of settlement money from the Doe defendants.

109. Once the Plaintiff had utilized the power of the courts to issue the subpoenas and obtain the Defendant's identifying information, this information was first used NOT to protect Plaintiff's copyrights by issuing a DMCA takedown notice, or by sending a cease-and-desist letter or by taking any other reasonable measure that would demonstrate a desire to protect its copyrights and mitigate its damages. Instead, an agent of Plaintiff acting in some unknown capacity contacted Defendant in an effort to prevail upon him to settle the matter out of court. Plaintiff expected that it would cost Defendant thousands of dollars to obtain legal counsel and respond to a lawsuit,

and Plaintiff anticipated and intended that the allegations of illegal conduct and the distasteful subject matter of such a lawsuit (namely, the pornographic nature of the films in question) would induce Defendant to settle quickly.

110. When Defendant refused to settle, Plaintiff filed the instant case, again avoiding the payment of multiple filing fees by joining three defendants in one case even though, according to Plaintiff's own information, the alleged actions (which Defendant has denied) took place on three distinct dates and times. As with the case filed against the 30 Does, there is no factual or legal basis for joining these three defendants in one action.

111. Thereafter, pressure to settle was still brought to bear in the form of phone calls, not from Plaintiff's attorney of record, but by Plaintiff's agent Anthony Palmer. Service of the Complaint was made on a weekend morning when Defendant's neighbors were known to be home and likely to observe. The Defendant's son answered the door and was upset because he thought the police had arrived. In all of these ways, Plaintiff and its attorney intended to bring pressure to bear upon Defendant so that he would not oppose the lawsuit, so that he would seek to avoid the embarrassment and cost of litigating against Plaintiff and pay Plaintiff a settlement.

112. Plaintiff's conduct of these two cases against the Defendant must also be viewed in the light of the fact that this is not an isolated incident. Plaintiff has proceeded in this very same way in hundreds of cases in fourteen different states, and has snagged thousands of Doe defendants in its net, regardless of guilt or innocence. Moreover, Plaintiff is part of a nationwide network of pornography companies all working with a single goal: use the Federal Court system to obtain financial settlements from internet subscribers through bullying and intimidation.

113. Plaintiff's attorney also represents Patrick Collins, Inc., which, upon information and belief, is essentially the same entity as Malibu Media LLC and is undeniably engaged in the same policy of mass copyright infringement litigation. Patrick Collins, Inc., has already been chastised and warned by this court regarding its use of the information it obtains from subpoenas in its Doe cases: "[t]he Court emphasizes that Plaintiff may only use the information disclosed in response to the [*3] subpoenas for the purpose of protecting and enforcing its rights as set forth in its Complaint. *The Court cautions Plaintiff that improper use of this information may result in sanctions.*" *Patrick Collins, Inc. v. Doe*, 2012 U.S. Dist. LEXIS 91249, 2-3 (D. Colo. June 29, 2012) (emphasis added).
114. Despite this warning in that case, Plaintiff's handling of the information disclosed in response to the subpoenas in this case was to use it for an improper purpose in violation of that Court's order. Specifically, this information was transmitted to a third party "call center" whose only apparent goal is to make repeated harassing calls, sometimes for months at a time, solely to pressure accused victims of this extortion scheme, like Defendant, into settling or else risk public embarrassment and damage to his or her reputation.
115. Defendant believes that such improper use should be sanctioned.
116. Plaintiff has failed to pay court filing fees which were due and proper based on the causes of action Plaintiff alleged.
117. Plaintiff has utilized this Federal Court in a manner which was intended to intimidate and harass the Defendant.
118. The Plaintiff's sole goal and motive is not a just and fair trial resulting in the preservation of any legal copyrights, but a swift extortion of money out of the pockets of an intimidated and embarrassed Defendant and other defendants like him.

119. Plaintiff will argue that it does not matter what its motives are where the end result is the same; that is, where it obtains monetary compensation for its allegedly infringed copyrights, it does not obtain some result which a defendant could not otherwise be compelled to do. However, when Plaintiff invokes the full force of the justice system, it must do so honorably and with clean hands; it must not do it with the intent to use the judicial process as a bludgeon to be wielded wildly. “The federal courts are not cogs in a plaintiff’s copyright-enforcement business model. The Court will not idly watch what is **essentially an extortion scheme**, for a case that plaintiff has no intention of bringing to trial.” *Malibu Media LLC v. John Does 1-10*, 2:12-cv-03623, Order, June 27, 2012, at p. 6 (emphasis added). This Plaintiff, like a schoolyard bully, has picked on thousands of victims and has used the judicial system as a mechanism to beat up on them. In such a case, Plaintiff’s motives do matter, very much.

120. There is no factual basis underlying Plaintiff’s claim against Defendant. Not only has Defendant not infringed any alleged copyrights Plaintiff may own, Plaintiff cannot prove any infringement based upon the allegations in the Complaint. All Plaintiff has alleged is that supposedly infringing activity took place through an IP address that may have been assigned to Defendant’s Qwest/CenturyLink account at a given time. As stated above, there are many possible explanations for why an IP address assigned to Defendant’s Qwest/CenturyLink account might have been collected by IPP Ltd.’s collection technology. This simple allegation stated in Plaintiff’s Complaint in no way ties Defendant to an intentional act of copyright infringement and Plaintiff knows this. Plaintiff knew it when it filed this suit, and Plaintiff knew it when it filed the Doe complaint against Defendant (1:12-cv-00402). Moreover, Plaintiff knew it when it filed the more than thirty suits it filed against hundreds of other Does in Colorado,

and Plaintiff knew it when it filed the hundreds of other cases against thousands of other Does all across the United States.

121. Further, when presented with evidence that the information Plaintiff relied upon was flawed and was, in fact, capturing innocent persons, Plaintiff and its attorneys chose to remain willfully ignorant of such facts in order to continue pursuing its business model.

122. There is no legal foundation for Plaintiff's claim against Defendant. Plaintiff has failed to allege the elements of either a direct or a contributory copyright infringement claim against Defendant. Rather, Plaintiff's Complaint is padded with generic statements about how BitTorrent downloads work and how copyright infringement *might* be done. There is nothing in the Complaint that can tie Defendant to an act of infringement besides the IP address, which, as noted, cannot be used to demonstrate any connection to any act of the Defendant whatsoever, let alone prove an intentional act of infringement.

123. The Copyright laws were never intended to be used in the manner in which Plaintiff is using them. Plaintiff is misusing and perverting the legitimate purpose and function of the Copyright laws through their for-profit litigation business model. A plaintiff legitimately seeking to protect its copyrights would not indiscriminately sue thousands of individuals across the nation in numbers which could not reasonably be handled by any attorney with no regard for whether those individuals had actually infringed upon the plaintiff's copyrights or not. A plaintiff legitimately seeking to protect its copyrights would not pursue cases knowing that it would be suing an innocent person – *at a minimum* – 30% of the time. A plaintiff legitimately seeking to protect its copyrights would not misrepresent to this court, as this Plaintiff did in 1:12-cv-00402, that the Doe defendants had copied Plaintiff's works and infringed its copyrights, thus tricking the court into allowing Plaintiff to issue subpoenas and

obtain personal identifying information about the Doe defendants which Plaintiff then used to obtain settlements from approximately 1/3 of those Does – with absolutely no proof of any wrongdoing by any of them. A plaintiff legitimately seeking to protect its copyrights would have made known to the court the flaws inherent in its IP address collecting technology and potential for errors. A plaintiff legitimately seeking to protect its copyrights would have accepted the offers from Doe defendants to inspect their computers or other proffers of evidence of innocence. Plaintiff has done none of these things.

124. The Defendant has been damaged in his personal and professional life by the conduct of the Plaintiff. Not only has he suffered from the stress, embarrassment and indignities of these lawsuits, and from the publication of these allegations by Plaintiff which expose him to public censure, shame and ridicule, his career has been negatively impacted because he has had difficulty when interviewing for employment and has lost job opportunities. Because prospective employers rely heavily on internet searches to find and verify information regarding applicants (see, **Exhibit K**, email from headhunter warning prospective job applicants to “clean up” their on-line image), the existence of this lawsuit is and has been incredibly injurious to Defendant. Defendant’s application for a loan to refinance his home mortgage was denied, and the specific reason given by the mortgage company was the existence of this lawsuit. **Exhibit L**.

125. Finally, all of the public allegations, harassing phone calls from a mass settlement “call center” and indeed the entire nationwide “campaign” are, on information and belief, based on knowingly inaccurate and/or false data that Plaintiff knew does not and would not identify the alleged downloader. Despite this malicious behavior and willful disregard for the judicial process, Plaintiff proceeded with this case with the intent and purpose of damaging Defendant.

WHEREFORE, the Defendant respectfully requests that the Court:

1. Find that these acts of Plaintiff amount to abuse of process;
2. Granting Defendant damages in the amount of \$1 million;
3. Granting the Defendant all fees and costs of suit;
4. For such other and further relief as the court may deem equitable and just.

COUNT II

INVASION OF PRIVACY

126. Defendant restates and realleges all of the allegations of the previous paragraphs as if more fully stated herein.

127. Plaintiff intentionally intruded upon Defendant's solitude, seclusion and private affairs by collecting data about the access individual IP addresses made of the internet without Defendant's knowledge, authorization, or permission.

128. Plaintiff intentionally intruded upon Defendant's solitude, seclusion and private affairs by forcing Qwest/Century Link to disclose the Defendant's identifying information through the issuance of the subpoena in Case No. 1:12-cv-00402-WYD. This information was subject to Defendant's reasonable expectation of privacy and was indeed protected by law such that Plaintiff had to obtain a subpoena (albeit by making false allegations) in order to obtain it. See *generally*, 47 U.S.C. § 551.

129. Plaintiff publicized false allegations – namely, the accusation that Defendant had illegally downloaded pornographic films – by placing them into a public document – namely, the Complaint against Defendant. This information is easily accessible to any interested person who searches Defendant's name through the Google search engine and/or any other search engine. In addition, since court documents are

public, all of Plaintiff's false allegations are available to the public through the court clerk's office.

130. The publication of these allegations is highly offensive to Defendant, as it falsely alleges illegal and distasteful activity on his part, and as such, would be highly offensive to any reasonable person.

131. The public can have no legitimate concern in hearing false allegations whose only purpose is to intimidate, embarrass and harass. Defendant is not a public official or a public figure in whom the public might have some legitimate interest.

132. The Defendant has been damaged in his personal and professional life by the conduct of the Plaintiff. If an individual uses the Google or Bing search engine to search Defendant's name, the first page has several entries that are all related to this lawsuit. This situation has existed since the lawsuit was filed in April and will continue for the foreseeable future so long as this lawsuit is ongoing, and moreover, it will continue for as long as Plaintiff continues its for-profit litigation business model across the country because that will keep attention upon Defendant even after his case is resolved.

133. Moreover, due to the nature of the internet, Defendant will continue to be damaged in the future by this lawsuit. Just as gossip continues to hurt and rumors continue to swirl whether there is any truth to them or not, these allegations will remain in the public consciousness and the public record long after this case is concluded.

134. The damage to Defendant's reputation has already been done simply by virtue of the allegation. This case is getting nationwide attention in media and on blogs, and it is clear that many individuals believe, simply because Defendant has been accused of downloading pornography, that he did it. See **Exhibit M**, screenshots: comments to Torrentfreak.com article regarding the First Amended Counterclaim: e.g., "I didn't

know he liked porn until he posted this lawsuit.”; *see also*, comments to reddit.com article on this case, *e.g.*, “For someone who has never downloaded porn in his life he sure knows a lot about this subject.”; *see also*, <http://betabeat.com/2012/07/man-sued-for-downloading-porn-sues-right-back/> (“He also denies that he has ever seen a pornographic movie in his entire life, which... if you say so, buddy.”) It is a well-known psychological principle that people tend to believe the first thing they see or hear, and that it is very difficult to later change their minds, no matter how erroneous that first information was, and no matter how much factual material one brings to bear against that first perception. These allegations, as soon as they were made by Plaintiff, began to do extraordinary damage to Defendant’s reputation and will continue to do so for as long as the internet exists. People have had and will continue to have very personal, very visceral, and frequently, very negative reactions to them. Defendant has been a coach of youth athletic teams for several years. In future years, when background checks are performed, the first item that appears is going to be a lawsuit involving the illegal download of pornography. It is unlikely that that will be acceptable to any youth athletic association.

135. Defendant has been hampered and damaged in his career, as alleged in great detail throughout this Counterclaim and incorporated herein by reference. He has received several calls from recruiters in the months since this case was filed but nothing has gone beyond the initial phone interview despite Defendant’s clear qualifications for and suitability for the job. This can only be due to the discovery by the recruiter of the distasteful allegations of Plaintiff’s Complaint. Because prospective employers rely heavily on internet searches to find and verify information regarding applicants (*see*, **Exhibit K**, email from headhunter warning prospective job applicants to “clean up” their on-line image), the existence of this lawsuit is and has been incredibly injurious to Defendant.

WHEREFORE, the Defendant respectfully requests that the Court:

1. Find that these acts of Plaintiff amount to invasion of Defendant's privacy;
2. Granting Defendant damages in the amount of \$1 million;
3. Requiring Plaintiff to pay for and take out an advertisement which shall run in the Denver Post and the Daily Camera and the Colorado Hometown Weekly, Louisville Edition, which advertisement shall be no less than $\frac{1}{4}$ of a page in size and shall be run in the primary news section of each newspaper in its Sunday edition (or in the case of Hometown Weekly, in one weekly edition), and which advertisement shall specifically retract the claims of the Complaint, acknowledge that Plaintiff wrongfully brought this lawsuit against the Defendant, state that this lawsuit was groundless, acknowledge that the Defendant has not infringed in any manner against the Plaintiff and that Defendant is innocent of any wrong-doing in this matter, and apologize to Defendant, with the stipulation that the exact language of the advertisement shall be subject to the review and approval of Defendant and/or his attorneys;
4. Granting the Defendant all fees and costs of suit;
5. For such other and further relief as the court may deem equitable and just.

COUNT III

DEFAMATION

136. Defendant restates and realleges all of the allegations of the previous paragraphs as if more fully stated herein.

137. By filing the Complaint in the instant matter, Plaintiff has made public false and defamatory statements about the Defendant, including but not limited to the allegations that Defendant has illegally downloaded movies that are protected by copyright, and that Defendant has downloaded pornographic movies.

138. Plaintiff acted with negligence as to the truth or falsity of these statements. The Plaintiff treats this Defendant, as it treats all its defendants, as a cash cow to be milked at will.

139. The statements are false because (1) Defendant has not ever downloaded any movies via BitTorrent; (2) Defendant has not ever downloaded any pornographic movies; (3) Defendant has not infringed upon Plaintiff's copyrights; (4) upon information and belief, Plaintiff's asserted copyrights to the movies in question are not valid; and (5) Plaintiff knew or should have known that just because it allegedly discovered potentially infringing activity tied to an IP address, that does not in any way prove who the individual is who did the infringing activity (if, indeed, there was any infringing activity at all).

140. As described in great detail above, Plaintiff knew or should have known all of the above facts before filing the present action with this court.

141. The allegations made by the Plaintiff in the Complaint subject to Defendant to scorn, distrust, ridicule, contempt and tend to harm his reputation. The allegations tend to lower him in the estimation of his peers, involving as they do, illegal and contemptible and distasteful activities.

142. The allegations made by the Plaintiff in the Complaint have a tendency to injure the Defendant's occupation, business or employment. In fact, the Defendant has already been hampered in looking for work. The instant action is one of the first items that appears on a search of Defendant's name in the Google search engine and it appears multiple times. This case is also one of the first items that appears on a search using the Bing search engine. Because prospective employers rely heavily on internet searches to find and verify information regarding applicants (see, **Exhibit K**, email from headhunter warning prospective job applicants to "clean up" their on-line image), the existence of this lawsuit is and has been incredibly injurious to

Defendant. These facts clearly have had and will continue to have a negative impact on the Defendant's reputation personally and professionally.

143. Anthony Palmer, the individual who contacted Defendant on behalf of Plaintiff several times, specifically told Defendant that he should "Google" himself to see that the lawsuit had been filed and find out facts about the case, thereby waiving any privilege that could be asserted. Clearly, Plaintiff intended that Anthony Palmer, as its representative, make Defendant aware of this very public exposure. Because prospective employers rely heavily on internet searches to find and verify information regarding applicants (see, **Exhibit K**, email from headhunter warning prospective job applicants to "clean up" their on-line image), the existence of this lawsuit is and has been incredibly injurious to Defendant.

144. The Defendant has been, and will continue to be, damaged in his personal and professional life by the conduct of the Plaintiff. Not only has Defendant suffered from the stress, embarrassment and indignities of these lawsuits, and from the publication of these allegations by Plaintiff which expose him to public censure, shame and ridicule, his career has been negatively impacted because he has had difficulty when interviewing for employment and has lost job opportunities. Because prospective employers rely heavily on internet searches to find and verify information regarding applicants (see, **Exhibit K**, email from headhunter warning prospective job applicants to "clean up" their on-line image), the existence of this lawsuit is and has been incredibly injurious to Defendant. Even if Plaintiff withdraws its Complaint, the detrimental effect of these allegations may linger for years.

145. Plaintiff should not be permitted to assert the defense of privilege to this claim because Plaintiff comes before this court with unclean hands and in bad faith. As already described in detail above, Plaintiff is part of nationwide epidemic, and Plaintiff has already been castigated and sanctioned by courts in California and New

York for its tactics. Plaintiff knew or should have known that it had no evidence tying Defendant to the alleged acts of infringement, and yet it brought this lawsuit with utter disregard for that fact. Moreover, upon information and belief, Plaintiff intentionally and willfully placed its works on the internet as a “honeypot” or authorized its agents and/or employees to do so, for the express purpose of luring potential infringers who could then be sued for infringement and bullied into a settlement. This lawsuit is not an isolated incident; it is part of a deliberate, calculated business plan.

WHEREFORE, the Defendant respectfully requests that the Court:

1. Find that these acts of Plaintiff amount to defamation;
2. Granting Defendant damages in the amount of \$1 million;
3. Requiring Plaintiff to pay for and take out an advertisement which shall run in the Denver Post and the Daily Camera and the Colorado Hometown Weekly, Louisville Edition, which advertisement shall be no less than ¼ of a page in size and shall be run in the primary news section of each newspaper in its Sunday edition (or in the case of Hometown Weekly, in one weekly edition), and which advertisement shall specifically retract the claims of the Complaint, acknowledge that Plaintiff wrongfully brought this lawsuit against the Defendant, state that this lawsuit was groundless, acknowledge that the Defendant has not infringed in any manner against the Plaintiff and that Defendant is innocent of any wrong-doing in this matter, and apologize to Defendant, with the stipulation that the exact language of the advertisement shall be subject to the review and approval of Defendant and/or his attorneys;
4. Granting the Defendant all fees and costs of suit;
5. For such other and further relief as the court may deem equitable and just.

COUNT IV

INTENTIONAL INFLICTION OF EMOTIONAL DISTRESS

146. Defendant restates and realleges all of the allegations of the previous paragraphs as if more fully stated herein.

147. In all Plaintiff's actions connected with the filing of both cases (*Malibu Media LLC v. John Does 1-30* and *Malibu Media LLC v. Fantalis, Dunn and Deus*), Plaintiff has acted with the specific intent to obtain a monetary settlement from every Doe at the lowest cost possible to Plaintiff.

148. Once again, Plaintiff's conduct in this specific case must be viewed in the light of Plaintiff's conduct in all of the cases filed in all of the Federal Districts: hundreds of cases with thousands of Doe defendants. In Colorado alone, Plaintiff's tally is already well over 500 citizens targeted in over 30 cases. Significantly, by lumping all of these Doe defendants together and not suing them individually, Plaintiff has saved more than \$150,000.00 in filing fees. At the settlement rate of 35% estimated by one IP "harvester," APMC (see Exhibit B), Plaintiff can expect approximately 163 settlements totaling anywhere from \$163,000 to \$500,000 or more, assuming settlements in the range of \$1,000 to \$3,000 which is on the low side. Or, if one uses the higher 50% settlement rate estimated by Plaintiff's own counsel in Florida (and the mastermind of Plaintiff's for-profit litigation business), Mr. Lipscomb, Plaintiff can expect anywhere from \$250,000 to \$750,000. Plaintiff reaps all this for an investment of less than \$10,000 in filing fees and a few hours of an attorney's time. This misuse of the Federal Courts is outrageous and extreme.

149. In the instant case, Plaintiff's first act after obtaining Defendant's identifying information was not to attempt to protect its copyrights through various legal means but to attempt to obtain a monetary settlement from Defendant. Moreover, Plaintiff's

counsel of record did not make the contact. Defendant has never once been contacted by Plaintiff's legal counsel regarding settlement, only by Anthony Palmer, a person who claims to represent Malibu Media and whose name has been tied to Patrick Collins, Inc., in connection with other, similar mass copyright suits of this type.

150. There is no way of looking at Plaintiff's scheme and calling it, as Plaintiff does, a legitimate means of enforcing its copyrights. Rather, as Judge Wright in the Central District of California portrays it, it is "essentially an extortion scheme." *Malibu Media LLC v. John Does 1-10*, supra, at p. 6.

151. In the instant case, Plaintiff alleges that Defendant downloaded pornographic films, the names of which would cause any reasonable person to cringe. Plaintiff's purpose and intent is to cause Defendant the emotional distress, shame and embarrassment that would naturally result from a list like this being associated with one's name, because by causing such emotional anguish, Plaintiff intends to motivate Defendant to pay a monetary settlement.

152. By accusing Defendant of downloading pornographic films, Plaintiff has in fact caused Defendant extreme emotional distress. By publishing these accusations through this lawsuit, Plaintiff has, in fact, caused Defendant extreme emotional distress, daily and ongoing anxiety, worry, and embarrassment. Defendant exists in a constant state of worry and fear over who will next discover these appalling – and false – accusations.

153. In the instant case, Plaintiff alleges that Defendant downloaded content from the internet illegally, which is offensive and damaging to Defendant's good name and reputation. Plaintiff's purpose and intent is to cause Defendant the emotional distress, outrage, humiliation, and damage to one's reputation that would naturally

result from such an allegation, because by causing such emotional anguish, Plaintiff intends to motivate Defendant to pay a monetary settlement.

154. By accusing Defendant of engaging in illegal internet downloads of Plaintiff's pornographic films, Plaintiff has in fact caused Defendant extreme emotional distress. Until one has been falsely accused of contemptible and illegal behavior, one cannot imagine the devastating emotional impact. But mere accusation was not enough for Plaintiff: Plaintiff had to make it public, exposing Defendant to contempt, humiliation and scorn among his friends, his community, his business colleagues, potential employers, and indeed, the entire world due to the broad reach of the internet. The screen shots and articles of Exhibit M are merely a small taste of what Defendant has had to face since this litigation was filed. This litigation has, in fact, caused Defendant extreme emotional distress, daily and ongoing anxiety, worry, and embarrassment. Defendant exists in a constant state of worry and fear over who will next discover these appalling – and false – accusations.

155. Since the inception of the first Doe lawsuit against Defendant in February, Defendant has been consumed daily by worry, anxiety, fear and stress due to Plaintiff's ruthless pursuit of him, an innocent victim. Further, Defendant feels outrage and anger at being victimized by Plaintiff along with so many other thousands of citizens across the country.

156. Because of these false allegations and the Plaintiff's outrageous and despicable handling of these lawsuits, the Defendant has suffered both personal emotional distress and damage to his professional reputation as alleged in prior counts and incorporated herein, which damage inflicts even more stress. Until one has been falsely accused of contemptible and illegal behavior, one cannot imagine the devastating emotional impact. Worst of all, no matter what the outcome of this case, these false allegations may cloud the Defendant's reputation for years to come.

WHEREFORE, the Defendant respectfully requests that the Court:

1. Find that these acts of Plaintiff amount to intentional infliction of emotional distress;
2. Granting Defendant damages in the amount of \$1 million;
3. Requiring Plaintiff to pay for and take out an advertisement which shall run in the Denver Post and the Daily Camera and the Colorado Hometown Weekly, Louisville Edition, which advertisement shall be no less than ¼ of a page in size and shall be run in the primary news section of each newspaper in its Sunday edition (or in the case of Hometown Weekly, in one weekly edition), and which advertisement shall specifically retract the claims of the Complaint, acknowledge that Plaintiff wrongfully brought this lawsuit against the Defendant, state that this lawsuit was groundless, acknowledge that the Defendant has not infringed in any manner against the Plaintiff and that Defendant is innocent of any wrong-doing in this matter, and apologize to Defendant, with the stipulation that the exact language of the advertisement shall be subject to the review and approval of Defendant and/or his attorneys;
4. Granting the Defendant all fees and costs of suit;
5. For such other and further relief as the court may deem equitable and just.

COUNT V

DECLARATORY JUDGMENT THAT DEFENDANT IS NOT LIABLE TO PLAINTIFF FOR COPYRIGHT INFRINGEMENT

157. Defendant restates and realleges all of the allegations of the previous paragraphs as if more fully stated herein.

158. Upon information and belief, Plaintiff created or caused and/or authorized its agents and/or employees to create a single digital file or website containing its films in order to lure potential infringers. This is known as a “honeypot” and it is done in order to trap infringers and, using the threat of infringement litigation as a weapon, to coerce them into a financial settlement.

159. By placing its films in a “honeypot” to lure infringers, Plaintiff explicitly and/or implicitly authorized the download, distribution and other use of its films.

160. Plaintiff is part of a nationwide scheme masterminded by a Florida attorney by which pornography companies make millions of dollars by tracking IP addresses, using call centers and/or settlement letters to pressure internet users – whose innocence is irrelevant to the pornography companies – into a settlement which is less expensive and less embarrassing than a public lawsuit, and then sharing the fees among the attorneys, the pornography companies and the tracking companies in arrangements that defy the Rules of Ethics governing the conduct of lawyers everywhere.

161. Upon information and belief, at no time did Plaintiff attempt to stop the download of its movies by removing them from the internet. In fact, by maintaining the films as a “honeypot,” it actively sought to encourage downloads in order to have more targets to extort money from.

162. Upon information and belief, at no time did Plaintiff attempt to mitigate its damages by removing the films from the internet. Again, by maintaining the films as a “honeypot,” it actively sought to encourage downloads in order to profit from infringement or allegations of infringement.

163. Upon information and belief, at no time did Plaintiff undertake to prevent any alleged infringers from continuing to infringe upon Plaintiff’s works, nor did Plaintiff attempt to prevent any alleged infringers from selling, distributing or otherwise using

Plaintiff's works. To Defendant's knowledge and belief, no DMCA takedown notices were issued, no cease-and-desist letters were ever sent, and no injunctions or restraining orders were ever sought.

164. Thus, upon information and belief, Plaintiff not only failed to prevent infringement of its allegedly copyrighted works, it actively encouraged that infringement in order to profit thereby.

165. The Plaintiff's claims in its Complaint are therefore barred by the equitable doctrines of unclean hands and estoppel.

166. Plaintiff has not established ownership of the copyright of the films listed in Exhibit B to Plaintiff's Complaint. Plaintiff has not produced the certificates of copyright ownership, only screenshots of the Copyright Office website.

167. Upon information and belief, Plaintiff does not own the full copyright of the films listed in Exhibit B to Plaintiff's Complaint. Rather, Plaintiff owns only the rights sufficient to bring lawsuits such as this one and the other lawsuits filed against the other Doe defendants. The only reason Plaintiff company exists is for the purpose of filing such lawsuits.

168. Plaintiff's claim to copyright is invalid due to the obscenity of the subject matter of the films.

169. Plaintiff's claim to copyright is unenforceable due to unclean hands, estoppel, fraud, obscenity and failure to timely and properly register.

170. Defendant did not download any of the films listed in Exhibit B to Plaintiff's Complaint, to which Plaintiff claims copyright.

171. Defendant has never downloaded any pornography whatsoever from the internet.

172. Defendant did not participate, at any point in time, in any BitTorrent that may have downloaded any works that Plaintiff alleges it owns the copyrights of.

173. Defendant did not engage in any conduct that infringed in any way upon any copyrights alleged to be held by Plaintiff.

174. Plaintiff has not alleged and cannot allege that Defendant copied constituent elements of its Works, because Defendant is not an IP address. If in fact constituent elements of Plaintiff's Works were transmitted through the IP address that was assigned by Qwest/CenturyLink to Defendant's account at a particular point in time (which is by no means certain, as demonstrated above), Plaintiff has made no factual showing as to why it is Defendant and not some other person – some hacker, some unauthorized user of his wireless network, or someone spoofing his IP address – who had infringed. In fact, Plaintiff cannot make such a showing and Plaintiff knows this.

175. Based on all the information stated herein, an actual and continuing controversy exists between Defendant and Plaintiff such that Defendant needs the court to declare the rights between the parties.

WHEREFORE, the Defendant respectfully requests that the Court:

1. Issue a declaratory judgment that Defendant has not infringed upon any rights that Plaintiff may have in the motion pictures listed in Exhibit B of its Complaint;
2. Issue a declaratory judgment that Defendant is not liable to Plaintiff for copyright infringement;
3. Issue a declaratory judgment that the Plaintiff has come before this court with unclean hands;
4. Issue a declaratory judgment that the Plaintiff has not mitigated damages;
5. Issue a declaratory judgment that the Plaintiff is estopped from asserting its claims against Defendant;

6. Issue a declaratory judgment that the Plaintiff failed to issue Digital Millenium Copyright Act (DCMA) takedown notices or otherwise seek to enjoin and prevent infringement of its works;
7. Issue a declaratory judgment that the Plaintiff not only failed to prevent the download of the works it now seeks to protect but rather encouraged and promoted said download in order to profit thereby;
8. Issue a declaratory judgment that the Plaintiff, its agents and/or employees have unlawfully and improperly instituted lawsuits not supported by facts or law and sought settlements of same, which constitutes misuse of copyright;
9. Granting the Defendant all fees and costs of suit;
10. For such other and further relief as the court may deem equitable and just.

COUNT VI

DECLARATORY JUDGMENT THAT PLAINTIFF'S WORKS ARE NOT ENTITLED TO THE PROTECTIONS OF UNITED STATES COPYRIGHT LAW

176. Defendant restates and realleges all of the allegations of the previous paragraphs as if more fully stated herein.

177. Article I, Section 8, Clause 8 of the United States Constitution reads as follows:

“To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.” From this Clause, all copyright and patent law springs. 150. Under this Clause, copyright is authorized only for works which promote the progress of science and the useful arts.

178. Plaintiff's works do not promote the progress of science.

179. Plaintiff's works do not promote the useful arts.

180. Upon information and belief, Plaintiff's works are hardcore pornography.

Defendant has never seen any of these films, but judging by the graphic nature of the titles listed in Exhibit B to Plaintiff's Complaint, there can be no doubt that these are pornographic.

181. In *Miller v. California*, 413 U.S. 15, 24 (1973), the Supreme Court stated that works which, "taken as a whole, appeal to the prurient interest in sex, which portray sexual conduct in a patently offensive way and, which, taken as a whole, do not have any serious literary, artistic, political or scientific value" are obscene.

182. Upon information and belief, Plaintiff's works depict obscene material. In other words, Plaintiff seeks to protect works which, (1) taken as a whole and judged by the average person applying contemporary community standards, appeal to the prurient interest in sex, and (2) portray sexual conduct in a patently offensive way as judged by the average person applying contemporary community standards, and (3) taken as a whole, do not have any serious literary, artistic, political or scientific value.

183. There is no protection under the First Amendment for works that are obscene. *Roth v. United States*, 354 U.S. 476 (1957).

184. It is a question of fact for the jury (or the judge, if sitting as a trier of fact) whether or not the works which Plaintiff attempts to protect with its alleged copyright registrations are obscene.

185. It is unsettled in the Circuit Courts, and has not been tested in the Supreme Court, whether obscene works can be copyrighted. It is a question of first impression in Colorado and in the 10th Circuit.

186. That illegal and immoral works have no right to legal protections is an ancient common law doctrine stretching back to 19th century England and the Rule in Priestley's Case.

187. Hardcore pornography is not speech by any definition of the term, nor is it protected expression under the First Amendment; it is obscenity. The fact that the sexual acts take place on film does not elevate them to the level of speech.

188. Upon information and belief, in order to create the works that are the subject of this lawsuit, Plaintiff and/or its agents and/or employees may have violated laws which prohibit pimping, pandering, solicitation and prostitution, including any and all claims of conspiracy to commit these acts. Thus, Plaintiff's works may depict criminal acts and/or conduct, and/or they may have come about as a result of criminal acts and/or conduct.

189. The illegal act of paying others to engage in sexual conduct so that one may watch is not protected speech if done in person; doing such illegal acts and filming it does not and should not elevate the request or the acts out of the realm of illegality or obscenity into the realm of protected speech.

190. Plaintiff's works are not copyrightable.

191. Based upon all of the information stated herein, an actual and continuing controversy exists between Defendant and Plaintiff such that Defendant needs this Court to declare the rights between the parties.

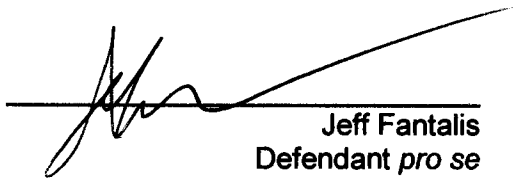
WHEREFORE, the Defendant respectfully requests that the Court:

1. Issue a declaratory judgment that each and every motion picture listed in Exhibit B of Plaintiff's Complaint is obscene;
2. Issue a declaratory judgment that each and every one of Plaintiff's motion pictures listed in Exhibit B of Plaintiff's Complaint are not entitled to copyright protection because they are obscene, because they do not promote the progress of science and the useful arts, and because they were created by and depict unlawful activity;
3. Striking Plaintiff's copyright registration of each and every motion picture listed in Exhibit B of Plaintiff's Complaint;
4. Finding that Plaintiff is not entitled to recover statutory damages and/or attorneys' fees;
5. Granting the Defendant all fees and costs of suit; and
6. For such other and further relief as the court may deem equitable and just.

DEMAND FOR A JURY TRIAL

Defendant-Counterclaimant hereby demands a trial by jury on all issues so triable.

Respectfully submitted,



Jeff Fantalis
Defendant *pro se*
818 Trail Ridge Drive
Louisville CO 80027
(303) 482-1211

Dated: August 24, 2012

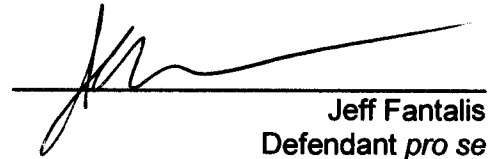
CERTIFICATION OF SERVICE

I, Jeff Fantalis, hereby certify that on August 24, 2012, I caused this Second Amended Answer and Counterclaim to be filed with the Clerk of the Court by U.S. Mail, Priority Delivery with Delivery Confirmation, at the following address:

Clerk's Office
Alfred A. Arraj United States Courthouse
Room A-105
901 19th Street
Denver, Colorado 80294-3589

On the same date, I served a copy of this Second Amended Answer and Counterclaim upon Plaintiff by mailing to Plaintiff's attorney of record, by U.S. Mail, Priority Mail with Delivery Confirmation, at the following address (with a courtesy email):

Jason A. Kotzker
Kotzker Law Group
9609 S. University Blvd. #632134
Highlands Ranch CO 80163
jason@jklgip.com


Jeff Fantalis
Defendant *pro se*

Dated: August 24, 2012

Subscribe | Contact Us

HOME OPINION WASHINGTON WHISPERS STEM DEBATE CLUB



Porn Companies File Mass Piracy Lawsuits: Are You At Risk?

So-called 'copyright trolls' are pulling internet data on movie downloads to sue for thousands in damages.

By JASON KOEBLER

February 2, 2012

Since the Recording Industry Association of America announced in 2008 that it would stop suing individual users for illegally downloading music, the high-profile piracy lawsuit has essentially disappeared. In its place, content producers—many of them in the pornography industry—have launched hundreds of quick-hitting lawsuits designed to get settlements from as many as 5,000 people at a time, advocates and defense attorneys say.

And by having a wireless internet connection, you're vulnerable.

The anonymous defendants—it's happened to more than 220,000 people since mid-2010—are accused of having illegally downloaded movies—from the porno "Stripper Academy" to the war film "The Hurt Locker"—using a peer-to-peer file sharing client called BitTorrent, lawsuit documents show.

[Opinion: Digital piracy is still a problem.]

The content producers (or their lawyers) log onto BitTorrent, download a movie, and mine other downloaders' easily-accessible internet protocol, or IP, addresses. A few weeks later those users will get an ominous letter from their internet service provider, saying a company has filed a subpoena requesting their identity, lawsuits allege.

The demands are usually the same: Pay a settlement of up to \$3,000 or face as much as \$150,000 in fines. Internet rights activists, such as the Electronic Frontier Foundation, have a name for these law firms and content providers: "copyright trolls."

"It's a common pattern at this point, they file lawsuits against hundreds or thousands of people at a time," says Corynne McSherry, intellectual property attorney at the EFF. People are liable as long as their internet connection was used—leaving anyone with a wireless connection vulnerable.

Many of the defendants in these cases say a stranger tapped into their Wi-Fi connection, something that can take only seconds if your connection is open, or a few minutes longer if a hacker uses one of the many Wi-Fi cracking programs available.

It happened to an IT professional, who wishes to remain anonymous, saying he was accused of downloading a pornographic movie about six months ago.

"I knew I didn't do it, I knew no one in my household did it," he says. "Your internet could have been used by neighbors, used by a guest."

"To carte blanche fire a shotgun in the air and say 'pay up' is just ridiculous," he adds.

His experience led him to create the blog DieTrollDie, a trove of information for people who find themselves accused of piracy. "It can be really scary and really confusing," he says of being subpoenaed.

[Should Congress Pass Anti-Online Piracy Legislation?]

His case was eventually dismissed, but he's learned a lot about what the "trolls" want: either your name (so they can sue you), or a quick settlement check. That makes fighting back difficult, because responding to the subpoena often requires defendants to identify themselves.

EXHIBIT A

"It's a fundamental Catch 22," McSherry says. "In a lot of places, by filing a motion to quash the subpoena, they have to identify themselves." And a lot of people are uncomfortable with their names being associated with downloading porn, whether they did it or not.

"No one wants to be associated with downloading something like [pornography]. That's going to make a lot of people extremely uncomfortable," McSherry says. That, she says, is why a lot of defendants end up paying the settlements.

Most of these cases end up eventually being thrown out, either because the company is going after people in the wrong district—it's not unusual for someone who lives in Maine to be sued in Washington, D.C.—or because the case links too many defendants together.

It's "preposterous," McSherry says, that 5,000 John Does were all working together in an elaborate piracy ring. "They sue them in one big lawsuit because it's convenient that way," she adds.

1 2 >

Tags:internet, technology, digital piracy

Copyright © 2012 U.S. News & World Report LP All rights reserved.
Use of this Web site constitutes acceptance of our Terms and Conditions of Use and Privacy Policy.

Subscribe | Contact Us

HOME OPINION WASHINGTON WHISPERS STEM DEBATE CLUB

ING DIRECT

Porn Companies File Mass Piracy Lawsuits: Are You At Risk?

So-called 'copyright trolls' are pulling internet data on movie downloads to sue for thousands in damages.

By JASON KOEBLER

February 2, 2012

It's also more convenient for a lot of the defendants to just pay up.

"A lot of people out there are paying the money because it's cheaper than getting an attorney. If you're rich enough, it's almost easier to write it off," the IT professional who was a victim of a piracy lawsuit says. "This is a cash cow, and the content trolls want to ride it out to the end."

- Is Internet Porn Destroying America?
- Founder of File-Sharing Site Arrested
- More technology news

jkoebler@usnews.com

Twitter: @jason_koebler

< 1 2

Tags:internet, technology, digital piracy

Copyright © 2012 U.S. News & World Report LP All rights reserved.
Use of this Web site constitutes acceptance of our Terms and Conditions of Use and Privacy Policy.

Anti-Piracy

Dear Sirs

Re: Business proposal - Combating piracy on peer to peer networks

APMC (Anti Piracy Management Company) has now been active several years in relation to unlawful file sharing of copyright material being carried out on the internet. We currently act for various clients, both in the UK, Germany, Asia, US and abroad, in respect of film, computer games and music titles. Of course, any copyright material can be subject to file sharing and the infringers pursued.

Evidence

The evidence is compiled by using IT experts who are based in Europe and the United States. They have the equipment to monitor, twenty-four hours a day/ 7 days a week, various file-sharing and BitTorrent websites for infringing usage. All the detection systems employed are verified by an independent court expert's report. Specific copyright titles can be tracked and the results limited to title.

Once the evidence is gathered, it is sent to the law firm in the jurisdiction in question so it can prepare an application to court for a disclosure order against the ISPs. Then the names and address relating to the IP addresses identified can be acquired. The ISPs (internet service providers) are entitled to charge their reasonable costs of complying with the order. The infringers are then written to and a demand for payment of damages and costs is made (together with the ISPs' costs). This can be in an amount of the client's choosing (within reason), subject to our guidance figure of around \$1,500. If payment is not forthcoming, proceedings are then commenced to obtain an order from the court, which can then be enforced against the infringer, if necessary, and also sent to other infringers, *pour encourager les autres*. (in order to encourage the others).

What are the prospects of success?

Ordinarily, we usually claim from each infringer an amount (depending on the copyright work involved) which is not unduly excessive, the aim being for the infringer to experience receiving an expensive, but affordable, "parking ticket" for his or her misdemeanor. We have found from our own experiences, and those of our German counterparts, that on average, around 25% of the infringers pay up after receiving our letter. Given we can handle a large number of addresses at any time (if the requisite number of "sources" are available), the deterrent effect (and revenue collected) can be quite substantial. Up to a further 10% tend to pay up once they have had their questions answered. We then commence cases against those who continue to default.

In Germany and in the UK, there have been test cases to establish the position in relation to specific defenses that infringers have raised and these have largely been successful. We are now embarking upon some in the US in order to produce the judgment mentioned above.

What are the benefits and costs?

Because of the way in which our IT experts provide the evidence it makes matters very cost-effective for the client. Not only does the client benefit from making it publicly clear that its copyright is not to be illegally exploited, it also dramatically reducing piracy of its products because of the deterrent effect created. There is usually a financial benefit from bringing the actions, for no initial outlay, which is obviously one of the main benefits of the program.

EXHIBIT B

Our proposal

Court orders

Our partner law firms have already been highly successful in obtaining a large number Court Orders. We are seeking to develop our network to enforce our client's copyright US-wide. As a result of this, full support will be provided to our partner law firms in terms of our experienced in-house counsel, consultancy, sample precedents to ISPs and draft motions. We only ask that our partners contribute to improving the source material we currently have by engaging with us in the disclosure process.

As we are steadily developing the reach of our operations as we require 3-4 law firms in each US state to obtain Court Orders for the disclosure of internet subscriber names and addresses. Our selected law firms will be remunerated with an agreed fixed fee plus a success fee for each Court Order obtained. We offer a steady stream of work throughout the year due to the high rate of infringements found by our IT Experts.

Letter sending

In each state we require at least one law firm to send out the letters of claim. If the law firm is willing to have a data processing company to assist with phone calls, letter sending and monies collected we would be willing to implement that into the program.

If you are interested in the above opportunity or require any further information, please do not hesitate to contact us by email on jc@apmcllc.com or by telephone on +1 323 522 5321. The next step is for us to schedule a conference call with you at a mutually suitable time to discuss our terms of engagement in more detail.

We look forward to hearing from you.

Best regards,

APMC LLC

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.

EXHIBIT C

Trace	Complaint type						Totals	
	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%80c%4B%24%28%86%9F%3B%D2%CC%BD%0A%D1%A7%BE%83%10v%peer_id=AZ2504-tUaIhr rpbVcq&port=55746&uploaded=0&downloaded=0&left=366039040&event=started&numwant=50&no_peer_id=1&compact=1&ip=A.B.C.D&key=NEBFoSCo'
```

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 re-

quest, 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. Enforce-

ment 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 real-time, 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://gulfoss2.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. Brodo, 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/>.

BaumgartenBrandt Attorneys at Law
Friedrichstr. 95-10117 Berlin

State Court Berlin
Littenstraße 12-17
10179 Berlin

Sekretary Ms. Haase
Direct dial +49 30 20 60 97 90-75
E-Mail haase@bb-legal.de
Our code 13/11/nli

Attorneys at Law

Dr. Ralf Baumgarten
Philipp Brandt
AndréNourbakhsh

Intern. Handelszentruin
Friedrichstraße 95
10117 Berlin

T+49 3 2 6 9 9
0 0 0 7 (1-0
F+49 3 2 6 9 90-
0 0 0 7 20

April 15, 2011

URGENT! Please submit immediately!

-16055/11

In the matter of the preliminary injunction

Guardaley Ltd. inter al. v. BaumgartenBrandt GbR

We substantiate our objection of 3/15/2011 as follows:

I. Facts

1. About the Parties

Petitioner No. 1 for the injunction* is a capital company with limited liability (Limited) under English law, formed on 4/24/2008.

Initial Proof: Extract from the Companies' House Register as

- Exhibit AG 1 -

It has maintained a branch in Germany in Karlsruhe since 1/29/2009.



Case 1:10-cv-12043-GAO Document 55-9 Filed 06/13/11 Page 2 of 18

Initial Proof: Commercial Register extract for Petitioner No. 1 as

- Exhibit AG 2 -

Petitioner No. 2 for the injunction*acts in commerce for Petitioner No. 1 as Director of Data Services.

Initial Proof: Affidavit of Petitioner No. 2 of 12/31/2009 before the United States District Court for the District of Columbia (File no.: CA. 1:10-cv-00453-RMC) in English as

- Exhibit AG 3 -

Respondent against the injunction* is a law office located in Berlin.

Attorney André Nourbakhsh (formerly Respondent No. 2 against the motion*) is an employee of the Respondent. In such capacity, he works at the address of the Respondent solely for the Respondent and does not pursue his own business activities there. Without limiting the generality of the foregoing, he is not a partner or managing director of the Respondent against the injunction.

2. Contractual Relationship between Petitioner No. 1 and the Respondent

There was a contractual relationship between Petitioner No. 1 and the Respondent, on the basis of which Petitioner No. 1 developed, and made administrative software available to Respondent for the duration of the contract.

In addition, Petitioner No. 1 entered into contracts with holders of copyrights for films. The subject of such contracts is the collection and documentation, for secure evidentiary purposes, of IP connection data of internet connection owners offering for download, in infringement of copyright, copyrighted works of clients of Petitioner No. 1 to other users, in a so-called peer-to-peer procedure (also called file-sharing). In this connection, it is denied, on the basis of lack of knowledge, that the Petitioner [sic] was also commissioned by its clients to investigate the IP data of owners of connections who merely attempted to download copyrighted works, without it being documented that the download was actually completed, much less that such works were offered via such connections for download, i.e., were publicly made available.

The Respondent also entered into contracts, for the provision of legal services, with copyright holders that had previously also entered into contracts with Petitioner No. 1 for the investigation of IP addresses. Respondent, in the context of its legal services, moves for orders to secure and reveal IP addresses of the connection owners behind the Internet service providers and asserts against such persons cease-and-desist and damages claims. Respondent is commissioned by its clients solely to proceed against such connection owners who make films publicly available, within the meaning of § 19 a of the Copyright Law, on the Internet, in infringement of copyright. It was not, and is not, commissioned to proceed against connection owners who merely attempt to download films, without offering the same to the public. For the motion to obtain the orders to secure and reveal pursuant to § 109 (9) of the Copyright Law, necessary to conduct the cease-and-desist proceedings, the Respondent presents to the respective court the Affidavit of Petitioner No. 2, in which Petitioner No. 2 declares that that only such IP addresses are identified as offering filmed works for download. He did not declare therein that Petitioner No. 1 investigates the IP addresses of persons who merely download filmed works or who have only attempted to do so.

Initial Proof: Affidavit of Petitioner No. 2 as

- Exhibit AG 4 -

Clients of Petitioner No. 1 were, and some still are, still clients of Respondent. Mr. Mark Damon, who is mentioned in the Affidavit of Ms. Barbara Mudge, represents, for example, the company Foresight Unlimited, located in the USA, and which at the time of the statements at issue in this

Case 1:10-cv-12043-GAO Document 55-9 Filed 06/13/11 Page 3 of 18

dispute was both a client of Petitioner No. 1 and a client of the Respondent. In order to comply with its obligations as attorneys pursuant to the service agreements with its clients pursuant to the Federal Attorneys' Regulation and the Regulation of Professional Responsibility, Respondent naturally continues to maintain contact with its clients, and thus with Mr. Mark Damon of Foresight Unlimited, irrespective of the existence of contractual relationships of clients of Petitioner No. 1.

3. Termination of the Contractual Relationship between Petitioner No. 1 and the Respondent

Respondent terminated, as of 1/21/2011, the contract between Petitioner No. 1 and the Respondent, without notice. The termination was sent to the Petitioner No. 1 and was received by the latter prior thereto by fax on 1/21/2011.

Initial Proof: Termination letter by the Respondent dated 1/21/2011 with transmission report of the fax transmission on 1/21/2011, 20:07 as

- Exhibit AG 5 -

In addition, as of 1/25/2011, Petitioner No. 1 declared to the Respondent, over the signature of Petitioner No. 2, the termination, without notice, of the of the existing contract. The termination was received by the Respondent by fax on 1/25/2011, at 14:37 and on 1/26/2011 by mail.

Initial Proof: Telefax of the Termination Letter of Petitioner No. 1 for the injunction dated 1/25/2011, 14:37

- Exhibit AG 6 -

Thus, the Petitioners knew, at least at the time of sending the motion for preliminary injunction to the State Court of Berlin, of the termination of the contract by the Respondent. While the motion for the issuance of the preliminary injunction is dated 1/21/2011, it was not received by the Court until 1/26/2011. The sending of the motion thus cannot have occurred prior to Tuesday, 1/25/2011. In fact, we allege that the Petitioners sent the motion for issuance of the preliminary injunction after 1/25/2011, 14:37, i.e., after receipt by Respondent of the termination by Petitioner No. 1. If the Petitioners are of a different view, then let them state and prove such.

To the extent the Petitioners in their motion for issuance of the preliminary injunction state that they were in a contractual relationship with the Respondent commencing in 2009, then the result is that they intentionally failed to state the fact that such contract had ended as of 1/21/2011. We expressly refer to the criminal law relevance of such false testimony.

4. Telephone Conversation between Mr. Nourbaksch and Ms. Barbara Mudge

a. Professional Position of Ms Barbara Mudge and Reason for Calling Her

Ms. Barbara Mudge is a member of the Board of Directors of the Independent Film and Television Alliance (IFTA) in Los Angeles, USA. She is responsible for companies from the film industry that are IFTA members. Included among such companies is, as can be seen from the text of the Affidavit of Ms. Barbara Mudge (Exhibit AS 3), Foresight Unlimited, represented by Mr. Mark Damon.

Ms. Mudge has also been active for some time as an employee of Petitioner No. 1.

Initial Proof: Email of Ms. Barbara Mudge of 2/25/2011 as

- Exhibit AG 7 -

Thus, Ms. Mudge was, and is, at no time a client of Petitioner No. 1, but rather its employee.

Case 1:10-cv-12043-GAO Document 55-9 Filed 06/13/11 Page 4 of 18

In addition, neither the Petitioners nor Ms. Barbara Mudge state, in the grounds of the motion or in the preliminary injunction, the background of the telephone conversation between Ms. Mudge and Mr. Nourbaksch. Ms. Barbara Mudge did not, as the grounds of the motion and the Affidavit might suggest, call Mr. Nourbaksch for no reason. Rather, the telephone call took place after the Respondent had called its client, Foresight Unlimited. Apparently, thereafter Mr. Mark Damon of Foresight Unlimited called Ms. Mudge. It is impossible for us to know whether Ms. Mudge was then speaking to Mr. Nourbaksch as a representative of Foresight Unlimited or in her capacity as an employee of Petitioner No. 1. In any case, the conversation took place at the desire, and on the initiative, of Ms. Mudge and with the knowledge of the client of the Respondent, Foresight Unlimited.

The information transmitted to Ms. Mudge in the conversation with Mr. Nourbaksch related solely to the client relationship between the Respondent and the client, Foresight Unlimited, and the telephone conversation previously conducted with Mr. Mark Damon. Ms. Mudge wanted to hear again for herself the questions raised therein. In this connection, reference was expressly and repeatedly made during the conversation to the conversation with Mr. Damon and Ms. Mudge repeatedly stated that Mr. Damon was her client and that she was, in her telephone call, complying with his request that she hear for herself what had been stated to him.

Initial Proof: Testimony of Mr. Nourbaksch, to be subpoenaed via the Respondent

The grounds for the motion and the Affidavit of Ms. Barbara Mudge also give the impression that Ms. Mudge was called on 1/5/2011 at the initiative of Mr. Nourbaksch. In fact it was Ms. Barbara Mudge herself who initially tried to call Mr. Nourbaksch on 1/5/2011, at ca. 16:30.

Initial Proof: Testimony of the employee of the Respondent, Ms. Nadine Haase, to be subpoenaed via the Respondent

Since Mr. Nourbaksch was not available at the time of Ms. Mudge's call, Mr. Nourbaksch as well as Mr. Philipp Brandt, Partner of the Respondent, called Ms. Mudge back on the same day.

Initial Proof: Testimony of Mr. Nourbaksch, to be subpoenaed via the Respondent

Ms. Mudge has incompletely and incorrectly represented the contents of the telephone conversation. At the time of making the Affidavit of 1/16/2011, and thus 11 days after the telephone conversation, Ms. Mudge was apparently unable to remember precisely the contents of the conversation. This is seen in the fact that she writes: "In gist, a telephone conversation with the following contents took place". Thereupon she provides „the gist“ of a summary of the contents of the conversation, abridged to the motion for the injunction and incorrectly and incompletely states what was said. In addition, the conversation was in English, and thus a foreign language for Mr. Nourbaksch. Moreover, the contents of the conversation were of a legal nature, as a result of which, Ms. Mudge, who unlike Attorney Nourbaksch, is not an attorney, could have misunderstood what Mr. Nourbaksch said.

That Ms. Mudge misunderstood the contents of the conversation, is seen with respect to the statement (which is no longer part of the dispute) in Point 1) of the Affidavit (Exhibit AS 3). Already in this Point Ms. Mudge incorrectly stated what was said: Mr. Nourbaksch informed Ms. Mudge that Petitioner No. 1 had, over a period of five months, transmitted to another law firm IP connection data that Petitioner No. 1 had collected for a copyright holder which was being legally represented by the Respondent. Such law firm had then, at the instigation of Petitioner No. 1, conducted, in the name of the copyright holder, copyright proceedings pursuant to § 101 (9) of the Copyright Law at various State Courts and had obtained appropriated orders for the disclosure of the data on the owners of the Internet connections. Mr. Nourbaksch informed Ms. Mudge that there was an exclusive client relationship between the copyright holder and the Respondent and the Petitioners did not inform the copyright holder of the transmission of the data to the third law firm. In contrast therewith, Ms. Mudge alleges in the Affidavit that Mr. Nourbaksch stated that legal titles had been obtained which had been assigned to the Respondent. The Respondent does not have rights assigned to it. It is also incomprehensible for Ms. Mudge to claim that Mr. Nourbaksch

Case 1:10-cv-12043-GAO Document 55-9 Filed 06/13/11 Page 5 of 18

claimed that the third law firm had instituted legal complaint.

b. As to the statements in the conversation that relate to the dispute

aa. As to Heading Point 1. a) — Theft of Software

In the telephone conversation at issue with Ms. Mudge, Mr. Nourbakhsch did not say that Petitioner No. 2 had stolen the investigation software used by Petitioner No. 1 from a Swiss company. Rather, Mr. Nourbakhsch merely informed Ms. Mudge about the circumstances of the previous employment of Petitioner No. 2 with Logistep AG. Specifically, he informed her that the Petitioner No. 2 had been employed until October 31, 2008, as Manager of the Technical Department of Logistep AG and that the latter had developed software for the investigation of copyright infringements. In an affidavit for a complaint in the USA against Petitioner No. 1 that has been published in the Internet Petitioner No. 2, however, claimed that he had been working for the Petitioner No. 1 since the beginning of 2007.

Initial Proof: Testimony of Mr. Nourbakhsch, to be subpoenaed via the Respondent

In addition, Mr. Nourbakhsch reported to Ms. Mudge that employees of Logistep AG had seen in the company car of Petitioner No. 2, during the latter's employment for Logistep AG, brochures and business cards of Guardaley Ltd.

Initial Proof: Testimony of Mr. Nourbakhsch, to be subpoenaed via the Respondent

Mr. Nourbakhsch expressly informed Ms. Mudge, that on the basis of the overall appearance of the circumstances, he could no longer, despite the long and good cooperation with the Petitioners, assume with certainty that Petitioner No. 2 had not, in the development of the software of Petitioner No. 1, had illegal recourse to the copyrighted know-how of Logistep AG. Mr. Nourbakhsch repeatedly emphasized that so far it was all only justified uncertainty, that the Respondent had, however, tried and was continuing to attempt to clarify the issue with Petitioner No. 1, in order to remove the doubts.

Initial Proof: Testimony of Mr. Nourbakhsch, to be subpoenaed via the Respondent

In addition, Mr. Nourbakhsch told Ms. Mudge, that Petitioner No. 2 was not willing, despite written demand by the Respondents, to dispel such uncertainties by making an affidavit.

Initial Proof: Testimony of Mr. Nourbakhsch, to be subpoenaed via the Respondent

Ms. Mudge failed to state all of these details in the Affidavit. She only reports what "stuck in her mind" after the telephone conversation of 11 days previously. And that is solely her own conclusion from the details of what was said, to wit, that the software had been "stolen".

bb. As to Heading Point 1.b) aa) — Undependable Research Service

Mr. Nourbakhsch indicated to Ms. Mudge that the Respondent had learned that the IP connection data determined by the Petitioner No. on the commission of the copyright holders was not 100% accurate. That the Petitioner No. 1 had included not only so-called uploaders, i.e., those offering works, but also persons who had made download inquiries to Petitioner No. 1. In addition, Mr. Nourbakhsch said that Petitioner No. 1 did not distinguish between up- and download determinations or did not mark them appropriately. The download inquiries were [verb missing...probably "designated"] as "Determinations", of which it was unable to be determined how many there were, without exception for civil law copyright claims without meaning. This meant that an unknown number of cease and

Case 1:10-cv-12043-GAO Document 55-9 Filed 06/13/11 Page 6 of 18

desist letters about copyright infringements might have been undertaken without a legal basis and that the Respondent did not have any way, either at that time, or today, of identifying such. Finally, Mr. Nourbakhsh indicated to Ms. Mudge that unjustified cease and desist letters could, in certain circumstances, result in damages claims of the persons receiving such letters against the copyright holders.

Initial Proof: Testimony of Mr. Nourbakhsh, to be subpoenaed via the Respondent

cc. As to Heading Point 1.b) bb) — Class Action in the USA Pending

Mr. Nourbakhsh indicated to Ms. Mudge that a class action complaint was to be found on the Internet, from which it could be seen that a plaintiff had instituted suit for himself as well as for 4,500 other affected persons against various parties, inter alia, Petitioner No. 1. He also informed her that the complaint was, on the basis of the grounds, based upon the accusation of “fraud and extortion”.

Initial Proof: Testimony of Mr. Nourbakhsh, to be subpoenaed via the Respondent

d. As to Heading Point 1. b) cc) — Offering Services by Others

In addition, the Affidavit of Ms. Mudge is incorrect to the extent that it claims that Mr Nourbakhsh offered to have investigations performed for “her clients” by another, specified company. The only correct aspect of this statement is that Ms. Mudge asked Mr. Nourbakhsh if there were other service providers as an alternative to Petitioner No. 1. Mr. Nourbakhsh answered this question by saying that there were numerous firms on the market. In response to the additional question by Ms. Mudge, as to whether and to what extent a change of service provider was possible, Mr. Nourbakhsh, in the context of his technical understanding, answered that the assumption of investigative activities by another firm was at least technically possible without problem.

5. In the Alternative: No Allegation of Untrue Facts

There would also be true facts in the statements forming the subject of the dispute. With respect thereto, individually:

a. As to Heading Point 1. a) — Theft of Software

It is claimed that, in the development of the software used for research by Petitioner No. 1, that the software was thus “stolen”. That the investigative software of Petitioner No. 1 is based on the knowledge of third parties can be concluded from the circumstances, particularly the circumstances relating to the employment of Petitioner No. 2.

In the judicial proceeding before the United States District Court for the District of Columbia, Petitioner No. 2 claimed, in an affidavit of 12/31/2009 (File No.: CA. 1:10-cv-00453-RMC) to have been employed since January 2007 for the Petitioner No. 1.

Initial Proof: Affidavit of Petitioner No. 2 before the United States District Court for the District of Columbia dated 12/31/2009 (File No.: CA. 1:10-cv-00453-RMC) in the English language, previously submitted as

- Exhibit AG 3 -

He was, however, employed at Logistep AG, with its offices in Steinhausen, Switzerland, in a managerial position as Chief Technical Officer, i.e., Manager of Technology. Thereafter, until 2/21/2009, he was an independent contractor for Logistep AG.

Case 1:10-cv-12043-GAO Document 55-9 Filed 06/13/11 Page 7 of 18

Initial Proof: 1. Affidavit of Mr. Richard Schneider, Member of the Administrative Board of Logistep AG, Sennweidstr. 45, 6312 Steinhausen, Switzerland as

- Exhibit AG 8 -

2. Testimony of Mr. Richard Schneider, Logistep AG, Sennweidstr. 45, 6312 Steinhausen, Switzerland

Logistep AG provides, as does Petitioner No. 1, services in the Internet and in the area of Internet security.

Initial Proof: 1. Commercial Register extract of Logistep AG as

- Exhibit AG 9 -

2. Affidavit of Mr. Richard Schneider, Member of the Administrative Board of Logistep AG, Sennweidstr. 45, 6312 Steinhausen, Switzerland, previously submitted as

- Exhibit AG 8 -

3. Testimony of Mr. Richard Schneider, Logistep AG, Sennweidstr. 45, 6312 Steinhausen, Switzerland

Logistep AG was one of the first companies to develop and use software for the collection, for secure evidentiary purposes, of IP addresses. Such software was developed by several Logistep AG employees over a period from February 2004 to May 2005 and has continuously been developed since then.

Initial Proof: 1. Affidavit of Mr. Richard Schneider, Member of the Administrative Board of Logistep AG, previously submitted as

- Exhibit AG 8 -

2. Testimony of Mr. Richard Schneider, Logistep AG, Sennweidstr. 45, 6312 Steinhausen, Switzerland

Petitioner No. 2 never disclosed to Respondent that he had worked for Logistep AG in the past, nor did he disclose that he had been employed by Logistep AG until October 31, 2008, and had worked with it until 2/21/2009 as an independent contractor.

According thereto, Petitioner No. 2, by his own statement, worked in a parallel fashion for Petitioner No. 1 in the same position, without disclosing this to Logistep AG.

Petitioner No. 2 also had, prior to his departure from Logistep AG his calls secretly forwarded from his office telephone number at Logistep AG to his cell phone number, 0176-24791824. He had the call forwarding installed, not on his telephone, but rather at the Logistep AG telephone services provider, so that the call forwarding would not be seen on the displays of the Logistep

AG telephones. The call forwarding was discovered by chance only on 4/29/2010 by Mr. Richard Schneider and Mr. Michael Wicher of Logistep AG.

Initial Proof: 1. Affidavit of Mr. Richard Schneider,
Member of the Administrative Board of
Logistep AG, previously submitted as

- Exhibit AG 8 -

2. Testimony of Mr. Richard Schneider, Logistep
AG, Sennweidstr. 45, 6312 Steinhausen, Switzerland

3. Affidavit of Mr. Michael Wicher, Mitarbeiter der
Logistep AG as

- Exhibit AG 10 -

In addition, Petitioner No. 2, while he was working for Logistep AG, had all emails directed to his email address achache@logistepag.com at Logistep AG forwarded to his private email address.

Initial Proof: Affidavit of Mr. Leszek Oginski, Direktor der
Logistep AG as

- Exhibit AG 11-

Finally, Mr. Oginski of Logistep AG saw brochures and business cards of Guardaley Ltd. In the company car of Petitioner No. 2, while he was still working for Logistep AG.

Initial Proof: Affidavit of theHerm Leszek Oginski, Director
der Logistep AG, previously submitted as

- Exhibit AG 11 -

Petitioner No. 2, however, offered, in the name of Petitioner No. 1, to the Respondent already on 12/10/2008, i.e., while he was still working for Logistep AG as an independent contractor, to collect data on internet connection owners who offer copyrighted works for downloading on the Internet.

Initial Proof: Email dated 12/10/2008 of Petitioner No. 2 as

Exhibit AG 12 -

In light of the fact that Logistep AG employed three employees for some 16 months in the development of its investigative software it is remarkable that Petitioner No. 1 was able, prior to the departure of Petitioner No. 2 from Logistep AG, to offer the same services as Logistep AG.

The doubts of Respondent as to the copyright status and above all as to the reliability of the „Observer" software were intensified by reason of the fact that Petitioner No. 2 contacted Mr. Nourbakhsch on 11/30/2011 by email and requested that the Respondent only use the expert opinion on the functionality and reliability of the “Observer” software only in critically necessary cases, without being able to state a credible reason therefor.

Initial Proof: Email of 11/30/2010 of Petitioner No. 2 as

- Exhibit AG 13 -

Case 1:10-cv-12043-GAO Document 55-9 Filed 06/13/11 Page 9 of 18

As a result of the aggregate impression of such facts, the Respondent began to have doubts about the copyright status of the "Observer" data collection software of the Respondents [sic {has to be "Petitioners"}]. The Respondent feared that Petitioner No. 2 could have had recourse to the know-how of his previous employer, Logistep AG, in the development of the investigative software used by Petitioner No. 1.

As a result, Mr. Nourbakhsch asked both Petitioners for a binding counterstatement in the form of an affidavit for the purpose of removing such misgivings.

Initial Proof: Email of Mr. Nourbakhsch of 1/12/2011, with attachments, as

- Exhibit AG 14 -

Both Petitioners refused, until making the motion for preliminary injunction, to make such an affidavit and thus to remove such doubts. All they did was inform the Respondent that they had transmitted the affidavits to a Mr. Guido Hettinger and that that the affidavits would be able to be executed „only after the completion of an outside examination".

Initial Proof: Email of Petitioner No. 2 dated 1/14/2011

- Exhibit AG 15 -

Only in the context of the motion for preliminary injunction did the Petitioners make such a statement.

b. As to Heading Point 1. b) aa) — Unreliable Investigative Services

Petitioner No. 1 is, as noted above, obligated and authorized to collect for the Respondent only the IP data of so-called uploaders, but not, that of persons who only engage in a so-called download or only inquire as to a download of copyrighted films. Commensurately, the Respondent only issues cease and desist letters against the upload, as making publicly accessible pursuant to § 19 a of the Copyright Law.

In January 2011, Respondent learned from ipoque GmbH that the investigative services being performed by Petitioner No. 1 were, in part, not what had been agreed upon with the copyright holders and did not correspond with the cease and desist letters and were thus unreliable.

ipoque GmbH is an IT firm that offers various services in the area of bandwidth and Internet management. The company is active internationally, inter alia, for various German universities.

Initial Proof: 1. Presentation of representative clients of ipoque GmbH under their Internet presence at <http://www.ipoque.com/company/customerreferences> as

- Exhibit AG 16 -

2. Testimony of Dr. Frank Stummer, to be subpoenaed via ipoque GmbH, Mozartstr. 3, 04107 Leipzig

One area, for which, inter alii, Dr. Frank Stummer is responsible, is the forensic data investigation of IP addresses where copyright infringements are occurring.

On the basis of the following incident, ipoque GmbH determined that Petitioner No. 1 collects IP data on owners of connections which are not making any films publicly available, which are thus not engaging in any "upload."

On 11/18/2009 at 01:03:25 CET, ipoque GmbH conducted a so-called test screening of the film „Antichrist" on the Internet. This film was being investigated at such time by Petitioner No. 1, on

Case 1:10-cv-12043-GAO Document 55-9 Filed 06/13/11 Page 10 of 18

Internet exchanges, especially Peer2Peer networks such „Bittorrent“, in the name of the copyright holder. The IP addresses collected by Petitioner No. 1 were identified by the Respondent in a proceeding pursuant to § 101 (9) of the Patent Law and a cease and desist letter sent to the owners of the connection pursuant to §§ 97, 19a of the Patent law, for the impermissible making publicly available of the aforementioned film.

In the course of such test screening, ipoque GmbH's software searched for the sources of illegal copies of the aforementioned film in the „Bittorrent“ network, i.e., searched for download possibilities from servers offering such files (uploaders). On the ipoque GmbH servers there was at this time, as at no other time, a complete or partial copy of the work “Antichrist”. For this reason, no part of the film “Antichrist” was offered in the „Bittorent“ network by ipoque GmbH, nor was this impression given on the Internet.

- Initial Proof:**
1. Testimony of the expert witness, Dr. Frank Stummer, to be subpoenaed via ipoque GmbH, Mozartstrafle 3, 04107 Leipzig
 2. Powerpoint presentation by ipoque GmbH “Facts about the Cease and Desist Letter for “Antichrist,” BaumgartenBrandt to ipoque, 11/18/2009” dated 1/13/2011 as

- Exhibit AG 17 -

Following the test screening, ipoque GmbH received a cease and desist letter, including an assessment of costs, from the Respondent, in which it was demanded that ipoque GmbH make a cease and desist undertaking by 5/18/2010. The accusation was of an upload constituting a copyright infringement, i.e., the making publicly available of the film „Antichrist” at the aforementioned time of the test screening.

- Initial Proof:**
1. Testimony of Dr. Frank Stummer, to be subpoenaed via ipoque GmbH, Mozartstral3e 3, 04107 Leipzig
 2. Cease and desist letter of 4/27/2010 to ipoque GmbH as

- Exhibit AG 18-

It is documented, as reliable evidence, that it is technically impossible for ipoque GmbH to have offered such a file in whole or in part, for a so-called “upload” to have occurred. It is also technically impossible for a download of the file to have occurred, which was not an accusation made in the cease and desist letter. At the time in question, there was contact with only one single third-party server on the part of ipoque GmbH, which this can only be attributed to Petitioner No. 1. But Petitioner No. 1, for its part, did not offer parts of the film. Rather, the Bittorrent monitoring program [of] Petitioner No 1 was set in such a way that it represented to other users, i.e., to their programs, by means of a falsified bit field, that it was always in possession of 50% of the file being sought, i.e., as to which inquiry was being made.

- Initial Proof:**
1. Testimony of the expert witness, Dr. Frank Stummer, to be subpoenaed via ipoque GmbH, Mozartstrafle 3, 04107 Leipzig
 2. Powerpoint presentation by ipoque GmbH “Facts about the Cease and Desist Letter for “Antichrist”, BaumgartenBrandt to ipoque, 11/18/2009” dated 1/13/2011 as

- Exhibit AG 17 -

For purposes of technical understanding, it should be explained that, as soon as a Bittorrent client

Case 1:10-cv-12043-GAO Document 55-9 Filed 06/13/11 Page 11 of 18

program of a user receives such a notice from another client program, it sends to the client of the other user a download inquiry for such file parts. Such an inquiry was sent at the time from the program (client) of ipoque GmbH to the server of Petitioner No. 1 and thereupon the IP address of the user, i.e., specifically the former IP address of ipoque GmbH's server, was recorded by Petitioner No. 1. That occurred even though ipoque GmbH neither offered an upload in infringement of copyright nor effected a download in infringement of copyright, because the server of ipoque GmbH could not receive any parts of the copyrighted file from the server of Petitioner No. 1, because they were not there.

- Initial Proof:**
1. Testimony of the expert witness, Dr. Frank Stummer, to be subpoenaed via ipoque GmbH, Mozartstrafle 3, 04107 Leipzig
 2. Powerpoint presentation by ipoque GmbH "Facts about the Cease and Desist Letter for "Antichrist,"BaumgartenBrandt to ipoque, 11/18/2009" dated 1/13/2011 as

- Exhibit AG 17 -

The consequence of this was that ipoque GmbH wrongfully received a cease and desist letter, on the basis of incorrect data collection.

After such cease and desist order became known, Petitioner had a meeting with ipoque GmbH's attorneys, as well as with Mr. Stummer. In the context of such meeting the aforementioned power point presentation (**Exhibit AG 17**) was shown to the Petitioners.

- Initial Proof:** Testimony of Mr. Dr. Frank Stummer, to be subpoenaed via ipoque GmbH, Mozartstral3e 3, 04107 Leipzig

Subsequently, Petitioners intentionally failed to disclose the entire contents thereof to the Respondent and to the clients of Petitioner No. 1. Only when the Respondent happened to have contact with ipoque GmbH in January 2011, did it learn that Petitioner No. 1 had made incorrect data determinations. After ipoque GmbH informed the Respondent by telephone that the monitoring services of Petitioner No. 1 were defective, employees of the Respondent, including Mr. Andre Nourbaksch and Mr. Christian Roloff traveled on 1/13/2011 to ipoque GmbH at its offices in Leipzig and had the course of the test screening explained to them, using the PowerPoint presentation that ipoque GmbH had already shown to Petitioner No. 1.

- Initial Proof:**
1. Testimony of Mr. André Nourbaksch, to be subpoenaed via the Respondent
 2. Testimony of Mr. Christian Roloff, to be subpoenaed via the Respondent

c. As to Heading Point 1. b) bb) — Class Action pending in the USA

Contrary to the allegation of Petitioners, a class action is pending in the USA against Petitioner No. 1. Mr. Dimitriy Shirokov, in his own name and in the name of 4,756 persons, instituted suit against Dunlap, Grubb & Weaver PLLC, US Copyright Group, Thomas Dunlop,

Nicholas Kurtz, Petitioner No. 1 and Achte/Neunte Boll Kino Beteiligungs GmbH & Co KG. The plaintiffs there are being represented by the law firm of BOOTH SWEET LLP in Cambridge, Massachusetts, USA..

Initial Proof: Class action by 4,756 plaintiffs against, inter alia, Petitioner No. 1, made available online under <http://boothsweet.com/wpcontent/uploads/2010/08/Master-Complaint1.pdf> by the law firm of BOOTH SWEET LLP, 32R Essex Street Studio 1A, Cambridge, MA 02139, USA, as

- Exhibit AG 19 -

The complaint was filed no later than 11/26/2010 at the United States District Court, District of Massachusetts. It has the file number 1:10-CV-12043-GAOt. On 11/26/2010, the court sent a notice to the defendants as to the fact that complaint had filed. The notice said: „A lawsuit has been filed against you".

Initial Proof: Notice of 11/26/2010 of the United States District Court, District of Massachusetts to the defendants as to the filing of a complaint

- Exhibit AG 20 -

The notice of the court also contained the demand to the defendants to answer the complaint within 21 days. In the system of prosecution of civil matters by the parties, the notice of the court of 11/26/2010 is sent to the defendants there by the attorneys of the plaintiffs. The Respondent has no knowledge of the extent to which the complaint has been received by Petitioner No. 1.

We assume that the Director of Petitioner No. 1, when he writes in his Affidavit (Exhibit AS 1) that a complaint of one individual person existed that the Petitioner No. 1 did not receive within 21 days, is referring to the complaint in **Exhibit AG 19**. In the complaint in **Exhibit AG 19** reference is made only to the „Plaintiff" in the singular; as one, however, can easily see when one reads the designation of the parties and Point 1 of the Introduction, Mr. Dimitriy Shirokov sued for injunctive relieve „on behalf of himself and all others similarly situated" and „on behalf of himself and 4,576 other similarly-situated victims" against, inter al., Petitioner No. 1. In addition, the complaint was filed and accepted as a „Complaint Class Action", i.e., a class action. Unlike in the Federal Republic of Germany, this is possible in the United States. Other complaints in the USA against Petitioner No. 1 were not able to be located on the Internet, where complaints have to be made available, by the Respondent. Die Petitioner No. 1 is politely requested, if it intends to maintain its allegation that a complaint by one single person existed, to submit the complaint of such single person.

At bottom, it is clear that a class action complaint by 4,576 persons is pending and that Mr. Nourbakhsh, in his statement that 4,300 persons had filed a class action complaint against Petitioner

No. 1, had actually understated the situation. The statement by the Director of Petitioner No. 1, Mr. Ben Perino, in the affidavit (Exhibit AS 1), that there had been at no time a class action complaint against Petitioner No. 1, thus is, in consequence, contrary to the facts.

6. Defective or Incomplete Service of the Order of 2/10/2011

The order of the State Court of Berlin of 2/10/2011 was neither delivered directly to Mr. Nourbakhsh nor was the order given to a person living or employed at the home address of Mr.

Case 1:10-cv-12043-GAO Document 55-9 Filed 06/13/11 Page 13 of 18

Nourbakhsh or deposited into the mail box at the home address of Mr. Nourbakhsh. Only the Respondent received a certified copy of the order, addressed to Mr. Nourbakhsh. This was deposited on 2/11/2011 in the mail box of the Respondent. The undersigned, however, have not appeared, either vis-à-vis the Court, nor vis-à-vis the Petitioners, as the procedural or trial representatives of Mr. Nourbakhsh.

The order of 2/10/2011 was deposited in the mail box of the Respondent, to wit on Friday, 2/11/2011 at its offices, but without the motion and the exhibits thereto.

II. Legal Considerations

1. **No Execution of the Preliminary Injunction**
 - a. **No Service of the Order upon Mr. Andre Nourbakhsh**

As a result of the failure to serve the order of 2/10/2011 upon Mr. Nourbakhsh, the order has not been executed vis-à-vis the latter, §§ 936, 929 (2) Code of Civil Procedure. The order was neither served upon him directly pursuant to § 191 Code of Civil Procedure, taken together with § 177 Code of Civil Procedure, nor as a substitute service pursuant to § 178 (1) No. 1 Code of Civil Procedure at the home of Mr. Nourbakhsh.

Depositing the order in the mail box of the Respondent does not constitute effective service upon Mr. Nourbakhsh. Service at the address of his professional activity, by placing in the mail box of the Respondent, was not possible as substitute service pursuant to § 178 (1) No. 2 Code of Civil Procedure, § 180 sent. 1 Code of Civil Procedure. The address of the Respondent is not the office of Mr. Nourbakhsh within the meaning of § 178 (1) No. 2 Code of Civil Procedure. An office within the meaning of § 178 (1) No. 2 Code of Civil Procedure is an area devoted to the business activity of the recipient of service (Baumbach/Lauterbach/Albers/Hartmann, [Commentary on the] Code of Civil Procedure, 69th ed., 2011, § 178 note 16; Federal Supreme Court {for non-constitutional matters} N[eue]J[uristische]W[ochenschrift]-R[echtsprechungs-]R[eport=New Legal Weekly –Case Report]** 2010, 489 (490) note 15). The recipient of service himself has to maintain a business office under the address (Federal Supreme Court, NJW 1998, 1958 (1959)). Since Mr. Nourbakhsh, as an employee, does not pursue his own business activities in the offices of the Respondent, as noted above, substitute service at the address of the Respondent is, for such reason, excluded.

Since there was not, prior to the substitute service, any attempt to effect service upon the recipient of the service personally, substitute service pursuant to § 178 (1) No. 2 Code of Civil Procedure, § 180 sent. 1 Code of Civil Procedure is also excluded.

Service pursuant to § 172 (1) Code of Civil Procedure was also not effectively made upon Respondent as the procedural representative of Mr. Nourbakhsh, since the Respondent was not, or [sic] is not, the procedural representative of Mr. Nourbakhsh. While the Respondent appeared as the representative of Mr. Nourbakhsh in the pre-trial cease and desist [matter], such appearance does not extend, however, to the judicial injunctive proceeding. The judicial proceeding commencing with the service of the preliminary injunction is, with respect to the pre-trial attorney correspondence about a cease and desist letter, a new phase and is to be distinguished therefrom (Superior State Court of Hamburg NJW-RR 1993, 958; Musielak, [Commentary on the] Code of Civil Procedure, 7th ed. 2009, § 172, note 2).

Since, however, the order was not executed vis-à-vis Mr. Nourbakhsh, he is no longer a party to the proceeding and can thus be heard as a witness. As the [Berlin] Superior Court has held, a party to a dispute who, while he was a party to the proceeding in the first instance, but, by reason of failure to appeal, is not a party to the appellate proceeding being pursued by the other parties to the dispute, may be heard as a witness (Superior Court [for Berlin], M[onatschrift für]D[eutsches]R[echt=Monthly Journal on German Law] 1981, 765). The Superior State Court of Koblenz held the same (Superior State Court of Koblenz, NJW-RR 2003, 283). The same

Case 1:10-cv-12043-GAO Document 55-9 Filed 06/13/11 Page 14 of 18

conclusion has to apply to the opponents of a motion for a preliminary injunction who are, as a result of failure to execute the injunction, no longer parties to the proceeding.

b. Service of the Order upon the Respondent without the Motion

The Petitioners have also not executed the injunction vis-à-vis the Respondent. To effect execution, there had to have been, in addition to the service of the order, a service of the motion as well, since the order of the LG Berlin of 10.02.2011 is, read alone, without the motion, not able to be understood.

Reference to the motion is made several times in the order. Thus, already in the decision as to costs, the calculation is made on the basis of the motion. The Respondent thus does not know to which points in the heading the partial amounts in controversy relate. In addition, in the grounds of the decision, on p. 5, 3rd paragraph, a position is taken on the partial prayer in 2.d) of the motion, without it being clear to the Respondent what prayer is meant, and what statement is supposed to be unfair pursuant to § 4 No. 10 Unfair Competition Law.

In cases where an order of injunction refers to the motion in the heading or even only in the grounds, the motion is to accompany the injunction (State Court of Wuppertal, Judgment of 3/18/2009, File No.: 3 O 480/08). This is all the more true, where the injunction refers to the motion and the injunction is not understandable when read alone (Superior State Court of Celle, Judgment of 2/3/1999, File No.: 2 U 279/98, juris [an online legal databank, similar to Lexis]).

2. No Claim for Injunctive Relief

a. No Competitive Relationship between the Parties

There is no competitive relationship between Petitioners and the Respondent. The characteristic of being a competitor pursuant to § 8 (3) Nos. 2 and 3 Unfair Competition Law is excluded at the outset in the case of the Respondent. The Respondent is, however, also not a competitor of the Petitioner pursuant to § 8 (3) No. 1 Unfair Competition Law. The fact that both Respondent and the Petitioner are active in the area of the pursuit of copyright infringements does not, by itself, permit the conclusion that they are competitors within the meaning of § 8 (3) No. 1 Unfair Competition Law. Competitors in the foregoing sense are solely businesses that attempt to market the same or similar goods or services within the same group of customers (Federal Supreme Court GRUR 2007, 884 note 35 — Cambridge Institute; Federal Supreme Court GRUR 2007, 1079 note 18 — Federal Printer; Federal Supreme Court G[ewerblicher]R[echtsschutz und]U[rheber]R[echt=Commercial Legal Protection and Copyright Law] 2009, 845 note 40 — Internet Video Recorder; Federal Supreme Court GRUR 2009, 980 note 9 — Email advertising II). It cannot be contended that the Respondent and die Petitioners offer the same or similar services. The Petitioners offer investigative services in the Internet. The Respondent offers, however, exclusively legal advice and representation. The fact that the services of both parties relate to copyright infringement does not change the distinction between such services.

b. Statement to Ms. Mudge neither an Allegation nor an Interference with Competitors

In the statements made to Ms. Mudge, there were neither facts within the meaning of § 4 No. 8 Unfair Competition Law alleged nor was a competitor interfered with pursuant to § 4 No. 10 Unfair Competition Law. Since Ms. Mudge is an employee of Petitioner No. 1, the statements made to her are to be attributed to the Petitioner [sic] pursuant to § 166 Civil Code] analogously.

Allegations pursuant to § 4 No. 8 Unfair Competition Law must be made, however, to third parties. The competitor affected by such allegation is not included in third parties in such sense. Allegations made to it are not capable of fostering or interfering with the sales or supplies of the business in question. This would only be true in the case allegations to persons who are not “in the camp” of the Petitioners.

The same applies to unfairness pursuant to § 4 No. 10 Unfair Competition Law. An interference is

Case 1:10-cv-12043-GAO Document 55-9 Filed 06/13/11 Page 15 of 18

excluded if it occurs [sic: I think what is meant is that the “allegations” are made, and thus occur, but not, obviously, the interference, which is being denied] as a result of allegations made to a business affected by the allegation. In such case, the allegation is not capable of resulting in an interference with the competitor.

c.No claim for Injunctive Relief for the Statements that are the Subject of the Dispute

aa. Evidentiary Value of the Affidavit of Ms. Barbara Mudge

In light of the abridged, “summarized in gist” and incorrect representation of the contents of the telephone conversation between Ms. Mudge and Mr. Nourbakhsch, the Affidavit of Ms. Mudge has no evidentiary value.

bb. As to the Allegation in Heading Point 1. a) — Theft of the Software

With respect to the statement under Point 1.a) of the heading, neither of the Petitioners have a claim for injunctive relief. The conditions of § 4 No. 8 Unfair Competition Law and § 823 (2) BGB, read together with § 186, 187 Criminal Code are not satisfied. Since Mr. Nourbakhsch never claimed that Petitioner No. 2 stole the software used by Petitioner No. 1, he did not publicize any untrue fact.

In all other respects, the statements of Mr.Nourbakhsch to Ms. Mudge as the representative, or at least the agent of, Foresight Unlimited, the client of the Respondent, were confidential statements, as to which the client of the der Respondent had a justified interest, § 4 No. 8, 2nd clause, Unfair Competition Law. Communication between attorney and client are subject, pursuant to § 43 a (2) Federal Attorney Regulation , to attorney confidentiality. At the European level, attorney confidentiality is protected pursuant to Art. 8 (1) European Human Rights Convention (protection of correspondence) read together with Art. 6 (1) and (3) letter c European Human Rights Convention (right to fair proceeding) as well as Art. 7 of the Charter of Basic Rights of the European Union (respect for communications) read together with Art. 47 (1), (2) sent. 2 and Art. 48 (2) of the Charter of Basic Rights of the European Union (right to advice, defense and representation, respect for rights of defense). The European Court of Justice has expressly confirmed the protection of attorney confidentiality (European Court of Justice in: NJW 1983, 503). Communications underlying attorney confidentiality is to be categorized as confidential and privileged. In addition, the confidentiality of the statement is a consequence of the fact that Mr. Nourbakhsch’s statements were made to only one recipient and not to a large number of recipients. Such communications are, in the view of the Federal Supreme Court, to be classified as confidential (Federal Supreme Court GRUR 1960, 135 (136) — Printing Orders).

Mr. Andre Nourbakhsch, as well as the client of the Respondent, Foresight Unlimited, also otherwise had a justified interest in the communication. To be considered, in a balancing of the interests, is, whether the person making the statement is legally or contractually required or obligated to communicate the facts (Kithler/Bornkamm, [Commentary on the] Unfair Competition Law, 29th ed., 2011, § 4, note 8.23). Mr. Nourbakhsch, as an attorney, commissioned and obligated to protect the interests of his client, Foresight Unlimited. This is a direct consequence of the statutory and contractual obligation of the attorney to notify and warn (Kleine-Cosack, [Commentary on the] Federal Attorney Regulation, 6th ed., Attachment I 1, § 11 Professional Regulation of Attorneys). Neglect of such obligations would have subjected the Respondent to a potential liability claim by its client. It is not only the right, but also the obligation, of the attorney to prevent such from the outset.

The interest of the client of the Respondent in the information constituting the subject of the dispute is, as a result of the large number of cases processed by using the „Observer” investigative software of Petitioner No. 1, is to be classified as very important.

cc. As to the Statement in Heading Point 1. b) aa) Unreliable Investigative Services

Nor, with respect to the statement under Point 1.b) aa) of the Heading, does either Petitioner have a claim for injunctive relief. Here as well, the conditions of § 4 No. 8 Unfair Competition Law

Case 1:10-cv-12043-GAO Document 55-9 Filed 06/13/11 Page 16 of 18

and § 823 (2) BGB read together with § 186, 187 StGB are not satisfied. Petitioner No. 1 provided unreliable investigative services, with the result that the statements forming the subject of the dispute are true facts.

In all other respects, here as well, Mr. Nourbakhsh's statements to Ms. Mudge, as representative of the client of the Respondent, Foresight Unlimited, constitute confidential communications, to which both the client of the Respondent and the Respondent have, for the same reasons, a justified interest, § 4 No. 8, 2nd clause Unfair Competition Law.

dd. As to the Statement in Heading Point 1. b) bb) — Pending Class Action Suit in the USA

Nor, with respect to the statement under Point 1.b) bb) of the Heading, does either Petitioner have a claim for injunctive relief. The conditions of § 4 No. 8 Unfair Competition Law and § 823 (2) BGB read together with § 186, 187Criminal Code are not satisfied. Mr. Nourbakhsh did not publicize any untrue facts.

As set forth above, a class action complaint in the name of 4,576 persons is pending in the USA against Petitioner No. 1. "Pending" means that the complaint has been filed with the court. "Legally pending" means that it has been served upon the defendant. Mr. Nourbakhsh did not say anything about legally pending, but rather only that a complaint was pending against Petitioner No. 1. The question of whether the complaint has been served upon the Petitioner No. 1 is thus not relevant for the decision.

In all other respects, here again, Mr. Nourbakhsh's statements to Ms. Mudge, as representative of the client of the Respondent, Foresight Unlimited, constitute confidential communications, to which the client of the Respondent has a justified interest, § 4 No. 8, 2nd clause Unfair Competition Law. We refer to the foregoing explanations.

ee. As to Heading Point 1. b) cc)

Point 1.b) cc) of the order of injunction is to be abrogated, due to lack of definitiveness, pursuant to § 253 (2) No. 2 Code of Civil Procedure . It is not clear, from the Heading, which contractual relationship is at issue. It is possible that the contractual relationship between Petitioner No. 1 and the Respondent is meant. But the Heading can also be interpreted to mean that the term "contractual relationship" means the contractual relationships between Petitioner No. 1 and its clients.

In addition, as a result of the reference in the Heading to the Affidavit of Ms. Barbara Mudge, it is not clear in what cases the Respondent is enjoined from contacting clients of Petitioner No. 1. Is contact for the purpose of offering cooperation without the assistance of Petitioner No. 1 only enjoined when one of the statements in Points 1. a), 1. b) aa) to cc) is made thereby, or only when all of such statements are made? Where, in the first case, is the substantive difference of the Heading in Point 1 b) cc) and the other Points of the Heading? Point 1. b) cc) of the Heading cannot be executed, due to lack of definitiveness.

If the term „contractual relationship" in Point 1. b) cc) of the Heading refers to the contract between Petitioner No. 1 and Respondent, then the claim for injunctive relief of Petitioner No. 1 under § 8 (1) read together with §§ 3, 4 No. 10 Unfair Competition Law fails, as a substantive legal matter, due to the fact that the contractual relationship between the parties was terminated as of 1/21/2011. The fact that the Respondent, following the termination of its contract with Petitioner No. 1, makes contact with the latter's clients, does not, by itself, result in unfairness pursuant to § 4 No. 10 Unfair Competition Law. Because luring away clients is in the nature of free competition, even when it is accomplished intentionally and systematically (on the basis of a plan) and the clients are still contractually bound to the competitor. As a result, objection can basically not be made when a business works to effect the dissolution of a contract in compliance with statutory or contractual provisions (termination, rescission or revocation periods) and takes advantage of the same for its own competitive purposes. Intruding into third-

party contractual relationships only becomes unfair when special circumstances are present (Köhler/Bornkamm, [Commentary on the] Unfair Competition Law, 29th ed., 2011, § 4, note 10.33, referring to Federal Supreme Court GRUR 1997, 920 (921) — Vending Machine Installers; Federal Supreme Court GRUR 2002, 548 (549) — Reimbursement of Car Rental Expenses; Federal Supreme Court GRUR 2004, 704 (705) — Departure Letter). Thus, if a sales representative who has left the company uses customer addresses that he has in his memory, this does not constitute anti-competitive behavior (Federal Supreme Court GRUR 1999, 934 (935) — Wine Consultant).

Even if there were a contractual relationship between Petitioner No. 1 and the Respondent, however, there would still be no claim for injunctive relief.

The fact that Respondent contacts possible clients of Petitioner No. 1 for the purpose of offering continued cooperation without the assistance of Petitioner No. 1, does not by itself result in unfairness. As set forth above, Ms. Barbara Mudge called Mr. Nourbakhsch at the order, or at least with the authorization, of a client of the Respondent, Foresight Unlimited, represented by Mr. Mark Damon. The knowledge of the contact data pertaining to Mr. Mark Damon was thus not based on the contractual relationship between the Respondent and Petitioner No. 1, but rather on the client relationship between Respondent and Foresight Unlimited. It is thus not true that the Respondent used customer addresses that had been entrusted to it or which it had obtained illegally, and thus resources to which it had no right. The instant case is not comparable with cases where employees approach customers of the employer, during the existence of the employment relationship, in order to obtain them as future customers for their own, or a third-party, business.

Irrespective thereof, the sole deciding factor is that the Respondent contacted only its own clients. That they are, or were, simultaneously customers of Petitioner No. 1, is irrelevant.

In addition, as previously set forth, Mr. Nourbakhsch in no way, either directly or indirectly, introduced or offered to the customers of Petitioner No. 1 services or business such as those of Petitioner No. 1.

On the basis of all of the foregoing, the preliminary injunction is to be abrogated.

In the event that the Court is of the view that the pleading of the Respondent is inadequate or needs to be supplemented, we request an appropriate notice from the Court. In such event, the Respondent will gladly supplement its pleadings extensively.

In the event that the Court requires a certified translation of **Exhibits AG 3, 19 and 20**, we also request a notice from the Court.

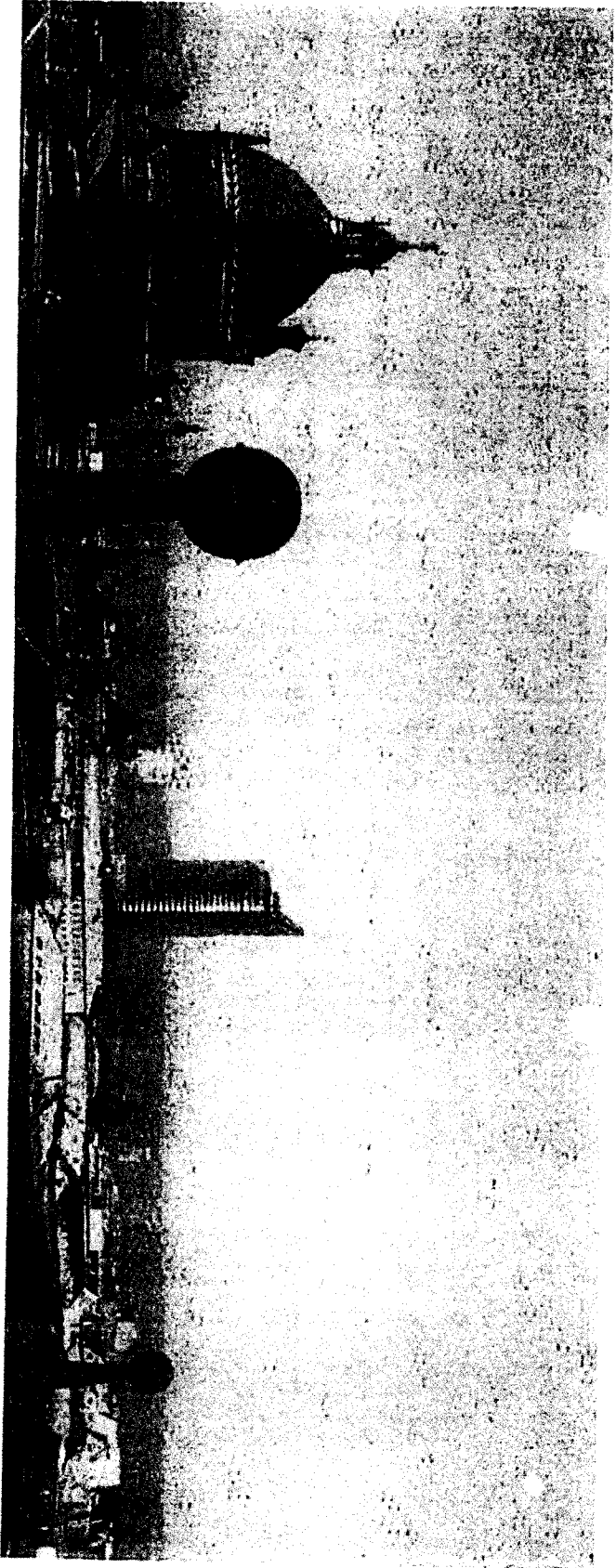
Service on the Petitioners shall be accomplished from attorney to attorney pursuant to § 174 Code of Civil Procedure .



Susanne Preuß
Attorney at Law

Exhibits

- AG 1 Extract from the Register of the Companies' House
- AG 2 Commercial Register extract for Petitioner No. 1
- AG 3 Affidavit of Petitioner No. 2 before the United States District Court for the District of Columbia of 12/31/2009 (File no.: CA. 1:10-cv-00453-RMC) in English
- AG 4 Affidavit of Petitioner No.2
- AG 5 Termination Letter of Respondent of 1/21/2011 with transmission report of the fax transmission on 1/21/2011, 20:07
- AG 6 Telefax of the termination letter of Petitioner No. 1 of 1/25/2011, 14:37
- AG 7 Email of Ms. Barbara Mudge of 2/25/2011
- AG 8 Affidavit of Mr. Richard Schneider, Member of the Administrative Board of Logistep AG
- AG 9 Commercial Register extract of Logistep AG
- AG 10 Affidavit of Mr. Michael Wicher, employee of Logistep AG
- AG 11 Affidavit of Mr. Leszek Oginski, Director of Logistep AG
- AG 12 Email of Petitioner No. 2 of 12/10/2008
- AG 13 Email of Petitioner No. 2 of 11/30/2010
- AG 14 Email of Mr. Nourbakhsch of 1/12/2011 with attachments
- AG 15 Email of Petitioner No. 2 of 1/14/2011
- AG 16 Presentation of reference customers of ipoque GmbH under their Internet presence at <http://www.ipoque.com/company/customer-references>
- AG 17 Powerpoint Presentation of ipoque GmbH „Facts on the Cease and Desist Letter about “Antichrist,” BaumgartenBrandt to ipoque, 11/18/2009” of 1/13/2011
- AG 18 Cease and Desist Letter to ipoque GmbH of 4/27/2010
- AG 19 Class Action Complaint of 4,576 plaintiffs against, inter al., Petitioner No. 1, available on line at <http://boothsweet.com/wp-content/uploads/2010/08/Master-Complaintl.pdf>, by the law firm of BOOTH SWEET LLP
- AG 20 Notice of the United States District Court, District of Massachusetts to the defendants as to the filing of a complaint, of 11/26/2010



**Facts on the Cease and Desist Letter “Antichrist,”
BaumgartenBrandt to ipoque, 11/18/2009**

CONFIDENTIAL
January, 2011

January 2011, CONFIDENTIAL

ipoque

Page 1

EXHIBIT E

**ipoque received a cease and desist letter for “Antichrist,”
which was in test screening**

Facts about the Cease and Desist Letter

Recipient of Letter: ipoque GmbH, Mozartstr. 3, 04107 Leipzig

Issuer: BaumgartenBrandt, Attorneys at Law, Berlin

Note: “Independent Security Provider” is Guardaley.

Client: Zentropa Entertainments23 Apps

Work: Film “Antichrist”

Date, Time: 1/18/2009, 01:03:25 CET

IP Address: 79.222.120.152

Note: At the time in question, a test screening with this film was running at ipoque for a third-party order. It was our IP address. It is a file in the BitTorrent Network (this information is not in the cease and desist letter).

Accusation: Offer to Download the Film by Release on the Hard Drive

Total Amount: 1,200.00 Euros

Deadline: 5/18/2010

The case is completely recorded and reproducible

Facts about the Cease and Desist Letter

The case was able to be completely reproduced.

This test screening was running on the PFS (Peer-to-Peer Forensic System), that ipoque itself uses for investigations of copyright infringements in Peer-to-Peer networks. As a result, we recorded and saved the entire traffic recordings; the case can thus be completely reproduced and demonstrated at any time.

We identified the other client (Guardaley)

The opposing investigators had the IP address 78.43.254.8 at the time in question. According to GoIP information, it is Baden-Württemberg Cable, Karlsruhe. In the period from 21:00 on 11/17/2009 to 02:00 on 11/18/2009, there were five different client hashes behind this IP address—one per file requested. At that time, we inquired about these files for Antichrist. This information is not in the cease and desist letter. We analyzed them from our investigation data bank:

ClientHash: 2D5554313831302D36D33E2627698192889A38D1
human readable: -UT1810-66%3E%26%27i%81%92%88%9A8SI
program and version: -UT1810-

The Guardaley client transmitted a characteristic bit field

Facts about the Cease and Desist Letter

We did not offer or upload.

Our client neither made an offer not did it upload, since, first, our P2P client informs all other clients that it does not have anything, and, second, the client could not upload anything. We demonstrably (in the complete traffic recordings) did not make a single transfer to this client.

The Guardaley client only inquired, but neither downloaded, nor sent us anything—ipoque also transferred nothing.

The clients of the opposing IP always transmit a bit field 0101010101010101... (they thus claim to have every other, and thus 50%, of the files).

Screen shot 1 shows this bit field.

Note: The screen shot was produced using Wireshark, an available program for the manual analysis of network traffic.

Screen shot 1: Bit field on the availability of pieces of the opposing client

At no time and in no direction did a transfer take place

Facts about the Cease and Desist Letter

Screen shot 2 is a seamless presentation of the complete occurrence resulting in the cease and desist letter.

1. It commences with the Handshake (Initiation of contact by the opponent)
2. TCP exchange (confirmation of the Handshake package, has nothing to do with the BitTorrent proceeding) → no BitTorrent transfer or the like takes place here, there is only an exchange to make and terminate the TCP connection
3. Confirmation of the Handshake by us
4. Opponent transmits (apparently falsified) bit field (see note above, Screen shot 1)
5. Our response that we are interested.
6. TCP (Confirmation of the Interested package from the previous step by the opponent)
7. Opponent requests a specific piece (although it knows that we do not have anything, since we sent no bit field — see note above)
8. TCP exchange (Confirmation of the request package by us)
9. Opponent again requests a piece
10. TCP (Confirmation of the request package by us)
11. TCP (Termination by us)
12. TCP (Confirmation by the opponent of the termination)
13. TCP (Termination by the opponent)
14. TCP (Confirmation by us of the termination)

Note: The screen shot was produced using Wireshark, an available program for the manual analysis of network traffic.

Screen shot 2: The complete proceeding resulting in the cease and desist letter

Steele | Hansmeier, PLLC
A leading anti-piracy law firm

July 13, 2011

VIA U.S. MAIL

Liuxia Wong
1180 Mahogany CT
Fairfield, CA 94553

Re: *Hard Drive Productions v. Does 1-48*
Case No. 3:11-cv-01957-JCS, Ref #5702

Dear Ms. Wong:

Steele | Hansmeier, PLLC has been retained by Hard Drive Productions Inc. to pursue legal action against people who illegally downloaded their copyrighted content (i.e., "digital pirates"). Digital piracy is a very serious problem for adult content producers, such as our client, who depend on revenues to sustain their businesses and pay their employees.

On March 28, 2011 at 12:33:00 PM (UTC), our agents observed the IP address with which you are associated illegally downloading and sharing with others via the BitTorrent protocol the following copyrighted file(s):

Amateur Allure - Jen

The ISP you were connected to: Comcast Cable

Your IP Address you were assigned during your illegal activity: 76.126.48.155

We have received a subpoena return from your ISP confirming that you are indeed the person that was associated with the IP address that was performing the illegal downloading of our client's content listed above on the exact date(s) listed above.

On April 22, 2011 we filed a lawsuit in United States Federal Court in the Northern District of California against several anonymous digital pirates (Case No. 3:11-cv-01957-JCS). Under the Federal Rules of Civil Procedure, our lawsuit against you personally will not commence until we serve you with a Complaint, which we are prepared to do if our settlement efforts fail. While it is too late to undo the illegal file sharing associated with your IP address, we have prepared an offer to enable our client to recover damages for the harm caused by the illegal downloading and to allow both parties to avoid the expense of a lawsuit.

Legal Correspondence – Settlement Purposes Only – Not Admissible Under FRE 408

Fax: 312.893.5677 | 161 N. Clark St. 4700, Chicago, IL 60601 | Tel: 312.880.9160
www.wefightpiracy.com

EXHIBIT F

Enclosed, please find a Frequently Asked Questions sheet, a payment authorization form and a sample of the Release that you will receive. We look forward to resolving our client's claim against you in an amicable fashion, through settlement.

Sincerely,

John L. Steele
Attorney and Counselor at Law

Enclosures

DECLARATION OF JOHN DOE

I, John Doe, hereby declare under penalty of perjury, pursuant to 28 U.S.C. § 1746(2) that the following statements are true and correct:

1. Approximately a year ago I received a phone call at my work from a person named Gerald Stern. Mr. Stern indicated that he was a representative of the law firm Lipscomb, Eisenberg & Baker, PL located in Miami Florida and that they had received information from my Internet Service Provider (ISP) through a subpoena request that my internet account had been linked -- through my alleged IP address -- to an act of unauthorized downloading of hardcore pornographic content through a BitTorrent program.
2. Mr. Stern indicated that I was involved in a lawsuit pending in Florida state court that involved copyright infringement and that this was a serious matter. Mr. Stern further informed me that his firm had sued people for this type of activity and had made anywhere from \$15,000 to \$30,000 per client.
3. Mr. Stern then proceeded to tell me that I probably wouldn't want to see my name in the "Denver Post" and that this could happen by the end of the week.
4. I informed Mr. Stern that I did not know anything about this and did not even know what a BitTorrent was.
5. Mr. Stern continued to inform me that that my network was wide open so that anyone could come into it and get information from it. Mr. Stern indicated that "we" could possibly be looking at a criminal charge of "exposing minors to pornography" which would result in a criminal case being filed against me.
6. Mr. Stern next told me that they (presumably the law firm) would be able to tell if I have been selling the copyrighted movie to others. Mr. Stern continued by telling me that if they are able to obtain my web surfing data from the data storage company (Latisys of Denver) they might be able to determine what other copyright materials I might have downloaded and sue me for that as well.
7. Approximately a year ago I also received a letter from Mr. Keith Lipscomb, of the law-firm Lipscomb, Eisenberg & Baker, PL located in Miami Florida. This letter indicated that an IP address that had been linked to my account through my ISP had allegedly downloaded hardcore pornographic content through a BitTorrent program without authorization. This letter indicated that my information had been subpoenaed by Mr. Lipscomb, and that I would be sued if I did not settle.
8. Based on personal investigation it appears that, Mr. Stern is not an attorney, but works for a "call center" that is associated with Mr. Lipscomb and Lipscomb, Eisenberg & Baker, PL and Jason Kotzker of Kotzker Law Group based in Highlands Ranch Colorado.

EXHIBIT 9

9. Based on personal investigation it appears that, names that are turned over from subpoena requests served on various ISP's from attorneys such as Mr. Lipscomb and Mr. Kotzker are transferred to this "call center" where settlement representatives continually call and attempt to pressure John Doe defendants into settling for several thousand dollars under the threat of a lawsuit and public embarrassment and threats of criminal actions.
10. I have been receiving harassing calls for approximately 5 to 6 months from similar representatives of Mr. Lipscomb and Mr. Kotzker. The harassing calls stopped for several months before beginning again. Many of the calls indicated that the law firm of Lipscomb, Eisenberg & Baker, PL, presumably through their representative counsel Jason Kotzker of Kotzker Law Group would file an individual lawsuit against me if I did not settle for several thousand dollars.
11. At no time was there presented an opportunity to provide evidence of innocence.
12. I have never downloaded any movies or other media content legally or illegally in my life.
13. I have never downloaded nor used any BitTorrent software in my life.
14. I have never financially benefited from anyone using my computer, nor have I ever encouraged anyone to ever download any movie or other content from any of my computers. If I was aware that such activity was taking place I would have done everything in my power to stop it.
15. I am providing this declaration anonymously out of a genuine fear of retaliatory litigation. My signature has been attested to by my attorney, David S. Kerr who is a member in good standing of the Colorado bar (#40947) and has been admitted to this Court. Mr. Kerr is further in possession of my personal contact information. Should this, or any Court wish for me to provide additional information I will do so under seal. In addition, should this, or any Court wish for me to provide live testimony I will do so at the Court's convenience.

s/ John Doe
John Doe

07/12/2012
Date

s/ David S. Kerr
Signature attested to by Counsel
David S. Kerr

07/12/2012
Date

From: "M. Keith Lipscomb" <KLipscomb@LEBFIRM.COM>
Date: Friday, July 1, 2011 2:50 PM
To: Brad Patrick <BradPatrick@baplegal.com>
Cc: copyright <copyright@LEBFIRM.COM>
Subject: RE: Copyright registrations?

Brad,

Our paralegals are currently drafting the complaints. These will be the first cases my clients' lawyers file in TX and AZ so it might take until Wednesday or Thursday to get a complaint on file in those 2 states. Copyright registrations are available online at the copyright office. You don't have to attach a certified copy or anything like that and instead we typically just attach a screen shot. My clients' lawyers, including me – check out the southern district CM/ECF, have already collectively filed over 50 federal cases in NY, CA, DC, MD, VA, NY, NJ, CO, FL and my clients have counsel in and new cases will soon be filed in NC, OH, PA. Further, we have counsel retained and could file and any moment cases in TX, AZ, IL, CT, GA. My clients are also negotiating agreements and interviewing lawyers in a long list of other states any one of which could be accelerated if needed. The federal suits we have filed to date all contain Doe numbers between 4 and 50. We frankly don't think it is much different to start a case against 1 Doe when we are already filing them against 4 Does.

As for registrations generally, please know some of my clients like Patrick Collins, Inc. and Kbeech, Inc. are U.S. studios. My U.S. clients universally register all their copyrights. Some of my other clients like Raw and Nucorp are foreign studios and their copyrights are enforceable under the Berne Convention. However, some of my foreign clients also register their copyrights in the U.S.

Registration is a red herring at this stage of the negotiating process, however, because it is not prerequisite to initiating suit if the work was created overseas. Further, it does not substantially change the risk-reward analysis for any of the parties. To explain, while registration is a prerequisite for the recovery statutory damages or attorneys' fees, actual damages are recoverable by someone suing under the Berne Convention. Here, my clients like RAW and Nucorp, are willing to enforce their rights in federal court because their actual damages are enormous and they have no choice, literally.

As for our actual damages being enormous please consider that infringers using the BitTorrent Protocol are liable for contributory infringement for each of the direct infringements that occur by subsequent infringers downloading the same torrent file. This is because the target Defendant knew or should have known of the infringement and the infringer aided the downstream infringers by sending the downstream infringers a piece of the copyrighted movie and/or by being in a network of computers from whom such an infringer could get a piece. Pleadings alleging contributory infringement through BitTorrent have universally withstood motions to dismiss.

Since a typical torrent file is downloaded 10,000s, if not 100,000s of thousands of times, the infringers' liability for the Plaintiff's actual damages is \$18 (the average cost of a movie) multiplied by the number of downstream infringers – use 25000 as a low ball average and you will get actual damages in the range of 450,000. Copyright law (which is just a branch of tort law) would then put the burden on the tortfeasor to sue everyone downstream for contribution. The liability for contributory infringement would not be limited to U.S. infringements. Indeed, the copyright act expressly prohibits sending copyrighted material overseas.

EXHIBIT H

To make this crystal clear for your clients, with 100% certainty, my clients, absolutely and without question, will file suit on Tuesday night in Florida and California and no later than Wed-Thur in TX and AZ if the motions are not withdrawn and the Does in the states where we have counsel don't come to the table in good faith. This is do-or-die time Brad. Your motions are impeding our ability to use the court system in a way that we believe we are legally entitled to do it. We cannot stand for that under any circumstances. Accordingly, the state court arguments have been teed up and to exert the maximum amount of pressure that we can we are filing to file individual federal suits to teach your clients the lesson that this is not the way to deal with us.

Here, the federal court suits have been standardized through filing and several stages beyond that. So, if they want to test me sooner, just pick a Doe in Florida, Colorado or California and say he is not going to settle today and that suit will be filed over the weekend. Please know, however, if we have to file suit, our settlement demands will increase. Toward that end, you should also apprise your clients that the average cost of a copyright litigation is 600K through trial, according to an AIPLA survey of fees in IP cases. This is a relatively simple case but the fees will nevertheless be substantial and indubitably in the 6 figures.

I guarantee you, my clients are 100% committed to taking their cases through trial and beyond, if necessary. Indeed, doing so is an anticipated part of this campaign and we are absolutely ready to do it now, if necessary and justified. Doing so against your clients is both necessary and justified in light of your motions and your clients failure to come to the table in good faith. I hope we can get past this and not have to waste any more our parties' resources but instead can reach an understanding where we negotiate in good faith. I am committed to doing that if you and your clients are as well.

I hope this answers your questions.

Best regards,

Keith

From: "M. Keith Lipscomb" <KLipscomb@LEBFIRM.COM>
Reply-To: "M. Keith Lipscomb" <KLipscomb@LEBFIRM.COM>
Date: Thursday, August 25, 2011 7:18 PM
To: Brad Patrick <BradPatrick@baplegal.com>, "M. Keith Lipscomb" <KLipscomb@LEBFIRM.COM>, copyright <copyright@LEBFIRM.COM>
Subject: Re: Settlement agreements

Welcome, and you can also tell your clients that IPP is one of three companies doing these scans and that they provided me with information which establishes several of your clients infringed movies from studios that I do not represent. In my individual suits, I am going to call all of those studios and have them become additional plaintiffs. Right now, statistically there is only about a .1 percent chance they'll get hit by these studios with a suit. Then I am going to go the other two companies that scan and get all the other plaintiffs I can from all of them.

If you want to save face with these clients and make your motion appear justified, tell them it caused me to send the emails I would send to ISPs. I will hold your original notices of withdrawal in trust until those emails are sent.

You can appear to be a hero or you can be obstinate and unreasonable. It's up to you. If your reasonable here, however, and another Omnibus motion gets filed, don't even bother trying to settle it.

Best regards,
Keith

Sent via BlackBerry by AT&T

EXHIBIT I



Law Enforcement Support
1801 California St, 10th Floor
Denver, Colorado 80202
303-896-2522
FAX: 303-896-4474

Michelle Thoms
Senior Security Specialist
Michelle.thoms@qwest.com
303-992-5802

February 27, 2012

Jeff Fantalis

818 Trail Ridge Dr
Louisville, CO 80027

Re: 201~~1~~²-00002338

Dear Ms. Fantalis:

It is Qwest's policy to notify our customers when we receive a subpoena requesting their records in a civil matter. Qwest protects its customers' privacy, but we are required to respond to lawful subpoenas for customer information unless otherwise ordered by the relevant court or regulatory body.

Qwest has been served with a subpoena in connection with the matter of: Malibu Media, LLC v. John Does 1-30, Case No. 1:12-cv-00402-WYD, United States District Court, District of Colorado. The subpoena requires Qwest to produce records and information related to your telephone/DSL account. Attached please find a copy of the subpoena issued to Qwest.

Qwest is required by law to respond to the subpoena and furnish the records requested on or before March 15, 2012.

If you have any objections to the subpoena, please notify me in writing of the objection as soon as possible, but no later than close of business on the above date. You will also need to file your objections with the court on or before the date specified to prevent the release of your records pursuant to the subpoena. If we do not receive a copy of your objections filed with the court by the above date, Qwest will produce the records as required by law.

If you have any questions, please contact me.

Sincerely,

M. THOMS
Qwest Communications

EXHIBIT J

4K 1/22/12 @ 3:45 pm

AO 88B (Rev. 06/09) Subpoena to Produce Documents, Information, or Objects or to Permit Inspection of Premises in a Civil Action

UNITED STATES DISTRICT COURT
for the District of Colorado

Malibu Media, LLC <p align="center"><i>Plaintiff</i></p>	Civil Action No. 1:12-cv-00402-WYD
v. John Does 1 - 30, <p align="center"><i>Defendants.</i></p>	

SUBPOENA TO PRODUCE DOCUMENTS, INFORMATION, OR OBJECTS OR TO PERMIT INSPECTION OF PREMISES IN A CIVIL ACTION

To: Qwest Communications
 c/o: The Corporation Company
 1675 Broadway, Suite 1200
 Denver, CO 80202

Production: YOU ARE COMMANDED to produce at the time, date, and place set forth below the following documents, electronically stored information, or objects, and permit their inspection, copying, testing, or sampling of the material:

Please produce documents identifying the name, address, and telephone number of the defendant John Docs listed in the below chart:

Doe#	IP Address	Date/Time UTC
22	174.22.132.59	1/22/2012 3:36
23	184.96.0.193	1/14/2012 5:14
24	184.99.247.212	1/18/2012 3:21
25	184.99.255.39	12/20/2011 5:58
26	67.41.140.20	12/8/2011 5:25
27	71.208.126.31	12/14/2011 12:22
28	71.208.248.113	1/16/2012 23:55
29	71.211.207.109	1/26/2012 1:56
30	75.166.112.233	11/20/2011 4:38

Place: Kotzker Law Group 9609 S. University Blvd., #632134 Highlands Ranch, CO 80163	Date and Time: APRIL 9, 2012 @ 9:30 a.m.

Inspection of Premises: YOU ARE COMMANDED to permit entry onto the designated premises, land, or other property possessed or controlled by you at the time, date, and location set forth below, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it.

Place:	Date and Time:

The provisions of Fed. R. Civ. P. 45(c), relating to your protection as a person subject to a subpoena, and Rule 45 (d) and (e), relating to your duty to respond to this subpoena and the potential consequences of not doing so, are attached.

Date: 2/22/2012

CLERK OF COURT

Signature of Clerk or Deputy Clerk

OR

JA [Signature]
Attorney's signature

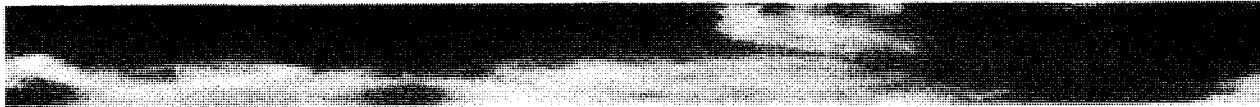
The name, address, e-mail, and telephone number of the attorney representing Plaintiff, who issues or requests this subpoena, are:

Jason Kotzker, Esq., The Kotzker Law Group, 9609 S. University Blvd., #632134, Highlands Ranch, CO 80163, Telephone: (303) 875-5386, Email: jason@KLGIP.com

Share

From the Desk of David Sterenfeld

August 2012



Hi Jeff,

The dog days of summer are here and the soaring temperatures out West are rivaled only by the sizzling JOB MARKET for Software SALES. We have been very busy with new job openings and placing numerous candidates in more sales and sales management positions than we have seen in over a decade. There continues to be a big demand from employers seeking professionals in all of these spaces: **Cloud Software - Security Software - SaaS Solutions - Social Media - Big Data and Analytics**. In this candidate-driven market where the competition is fiercer than ever, it is highly beneficial for a candidate to be presented by a well-connected Recruiter to get your name in front of the right hiring manager. Please contact me if you or your colleagues are considering a career move, or when your organization is looking to expand.

VISIT OUR WEBSITE



Before you are contacted by **CORPORATE DYNAMIX** for that coveted interview, we'd like to pass on some of our tips for winning interviews...Whether you are going on your first interview or your tenth, careful preparation is a must. Follow our tips for success:

- **Clean up your online image.** All employers routinely turn to the Internet to research potential hires, so it's important you have and maintain a professional online presence. Our last newsletter talked about using Facebook properly. Create a LinkedIn profile and keep your Facebook and Twitter accounts and personal ones separate. Before applying for a job, search for yourself online and see what appears. This way you can change or remove personal or unflattering content, by adjusting privacy settings or deleting items.
- **Do research.** When you interview for a job, the goal is to "sell yourself." Conduct research on the company beforehand so you can share w

Read what

EXHIBIT K

AVERE LENDING GROUP



Real Estate Lending

July 24, 2012

Jeff and Maryanne Fantalis
818 Trail Ridge Drive
Louisville, Colorado 80027

Regarding: Refinance - 818 Trail Ridge Drive, Louisville, Colorado 80027

Dear Jeff and Maryanne,

Please be advised that after submission of your loan application and documentation to the Bank, the Bank is unable to find any Investors willing to purchase your loan subsequent to closing, and is therefore unable to proceed with your refinance at this time due to the impending law suit that has been filed against you by Malibu Media, LLC.

Should the law suit be resolved, dropped or settled, I will be able to immediately resubmit your loan application and your refinance should easily be granted. There are no other issues with regard to your loan application that I have any concerns about other than this suit.

I am sorry that we cannot move forward at this point with your refinance. Please let me know if your status changes with regard to the law suit and I will get your loan resubmitted to the Bank.

If you have any questions, please do not hesitate to contact me.

Respectfully,

Teri A. T. Vanderhyden

Teri A. T. Vanderhyden

EXHIBIT L

Notice of Action Taken

Date Action Taken: 07/24/2012

Applicants: Jeff Fantalis
Address: 818 Trail Ridge Drive
 Louisville, CO 80027

Loan Amount: \$ 335,000
Interest Rate: 2.875 %
Term: 180 months

File No. : 14618292

Thank you for your application for:

Based upon your Mortgage Application for a loan we must inform you that:

Notice of Credit Denial:

We are regrettably unable to approve your request. Our principal reasons for this decision are indicated below.

Part I - Principal Reason(s) for Credit Denial, Termination, or Other Action Taken Concerning Credit.

In compliance with Regulation "B" (Equal Credit Opportunity Act), you are advised that your recent application for credit has been declined/terminated/changed. The decision to decline/terminate/change your application was based on the following reason(s):

- | | | |
|---|---|--|
| <p>A. CREDIT</p> <p><input type="checkbox"/> No Credit File</p> <p><input type="checkbox"/> Insufficient Credit Reference</p> <p><input type="checkbox"/> Insufficient Credit File</p> <p><input type="checkbox"/> Unable to Verify Credit References</p> <p><input checked="" type="checkbox"/> Garnishment, Attachment, Foreclosure, Repossession or Suit</p> <p><input type="checkbox"/> Excessive Obligations</p> <p><input type="checkbox"/> Insufficient Income for Total Obligations</p> <p><input type="checkbox"/> Unacceptable Payment Record on Previous Mortgage</p> <p><input type="checkbox"/> Lack of Cash Reserves</p> <p><input type="checkbox"/> Delinquent Credit Obligations</p> <p><input type="checkbox"/> Bankruptcy</p> <p><input type="checkbox"/> Information From a Consumer Reporting Agency</p> | <p>C. INCOME</p> <p><input type="checkbox"/> Insufficient Income for Mortgage Payments</p> <p><input type="checkbox"/> Unable to Verify Income</p> <p>D. RESIDENCY</p> <p><input type="checkbox"/> Temporary Residence</p> <p><input type="checkbox"/> Too Short a Period of Residence</p> <p><input type="checkbox"/> Unable to Verify Residence</p> <p>E. INSURANCE, GUARANTY or PURCHASE DENIED BY:</p> <p><input type="checkbox"/> Department of Housing and Urban Development</p> <p><input type="checkbox"/> Department of Veterans Affairs</p> <p><input type="checkbox"/> Federal National Mortgage Association</p> <p><input type="checkbox"/> Federal Home Loan Mortgage Corporation</p> | <p>F. OTHER</p> <p><input type="checkbox"/> Insufficient Funds to Close the Loan</p> <p><input type="checkbox"/> Credit Application Incomplete</p> <p><input type="checkbox"/> Inadequate Collateral</p> <p><input type="checkbox"/> Unacceptable Property</p> <p><input type="checkbox"/> Insufficient Data - Property</p> <p><input type="checkbox"/> Unacceptable Appraisal</p> <p><input type="checkbox"/> Unacceptable Leasehold Estate</p> <p><input type="checkbox"/> We do not grant credit to any applicant on the terms and conditions you have requested.</p> <p><input type="checkbox"/> Withdrawn by Applicant</p> |
|---|---|--|
- B. EMPLOYMENT STATUS**
- Unable to Verify Employment
- Length of Employment
- Temporary or Irregular Employment, Insufficient Stability of Income

Part II - Disclosure of use of information obtained from an outside source.

This section should be completed if the credit decision was based in whole or in part on information that has been obtained from an outside source.

Our credit decision was based in whole or in part on information obtained in a report from the consumer reporting agency listed below.

You have a right under the Fair Credit Reporting Act to know the information contained in your credit file at the consumer reporting agency. The reporting agency played no part in our decision and is unable to supply specific reasons why we have denied credit to you. You also have a right to a free copy of your report from the reporting agency, if you request it no later than 60 days after you receive this notice. In addition, if you find that any information contained in the report you receive is inaccurate or incomplete, you have the right to dispute the matter with the reporting agency.

Applicant: **Jeff Fantalis**

Name: _____
Address: _____
[Toll-free] Telephone number: _____

We also obtained your credit score from this consumer reporting agency and used it in making our credit decision. Your credit score is a number that reflects the information in your consumer report. Your credit score can change, depending on how the information in your consumer report changes.

Your credit score: _____ Date: _____
Scores range from a low of _____ to a high of _____

Key factors that adversely affect your credit score:

Number of recent inquiries on Credit Report: _____

Our credit decision was based in whole or in part on information obtained from an affiliate or from an outside source other than a consumer reporting agency.

Under the Fair Credit Reporting Act, you have the right to make a written request, no later than 60 days after you receive this notice, for disclosure of the nature of this information.

If you have any questions regarding this notice, you should contact:

Creditor's name: **TJJD, LLC d/b/a Avere Lending Group**
Creditor's address: **699 Tamarisk Court, Louisville, CO 80027**
Creditor's telephone number: **303-666-7322**

Our credit decision was based in whole or in part on:
File is being denied since the borrower is party to an open lawsuit. Unable to offer financing until the lawsuit has been settled or withdr

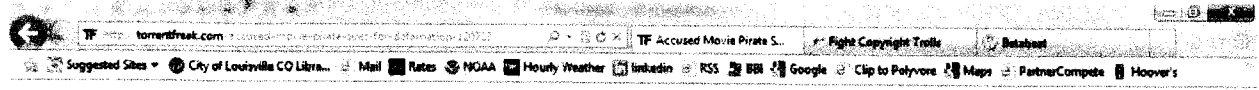
Notice: The Federal Equal Credit Opportunity Act prohibits creditors from discrimination against credit applicants on the basis of race, color, religion, national origin, sex, marital status, or age (provided the applicant has the capacity to enter into a binding contract); because all or part of the applicant's income derives from any public assistance program; or because the applicant has in good faith exercised any right under the Consumer Credit Protection Act. The Federal Agency that administers compliance with this law concerning this creditor is:

This notification is given by us on behalf of: **TJJD, LLC d/b/a Avere Lending Group**
699 Tamarisk Court, Louisville, CO 80027
303-666-7322

By: 
Colleen McAdams

Delivery Type: Mailed E-Mailed Hand Delivered

Delivery Date: **07/24/2012**



Anon1 1 day ago

It's about time someone fights back rather than settling to these blatant extortion schemes. If he gets an impartial judge and a half decent lawyer he'll be able to win, and it will set a precedent for future cases. More people follow suit and fight, the trolls lose even more money when they thought they could get an easy settlement. Insert snowball effect and the trolls will be running away with their tails between their legs.

As for not ever downloading an adult movie...hah, sure you haven't.

1 person liked this Like Reply



JordanKratz 1 day ago

Good Luck To You !!!

This is a worthy cause and I hope it happens.

Like Reply

The Guy 1 day ago

A shining example of fighting the power. I wish this fellow all the luck in the world. If this succeeds, it could be our saving grace to mounting massive counter-suits against these copywriting extremists.

1 person liked this Like Reply

Anon 1 day ago



Damn right! Sue the hell out of them!

I wish best of luck to that dude, grinet, EasyMONEYQMake

2 people liked this Like Reply



Boondoggie 13 hours ago

I didn't know he piked porn until he posted this lawsuit. Will he sue himself for defamation now too?

Flap

Like Reply

Real-time updating is paused. (Resume)

Add New Comment

Optional: Login below.

Type your comment here

Post as...



EXHIBIT M

Discussion thread on Reddit, 7/24-25/12

http://www.reddit.com/r/technology/comments/x210k/accused_porn_movie_pirate_countersues_for/

The screenshot shows a browser window with a Reddit page. The address bar contains the URL: http://www.reddit.com/r/technology/comments/x210k/accused_porn_movie_pirate_countersues_for/. The browser's toolbar includes various utility icons like Mail, Rates, NOAA, Hourly Weather, LinkedIn, RSS, BBI, Google, and Maps. The page content shows a discussion thread with several comments. The first comment, by user 'redbulence928', asks if copyrightability is directly related to free speech. A reply by 'player111' states that copyrightability is not directly related to free speech and that copyright covers a lot of things protected by free speech. Another comment by 'pyatrell' notes that someone who has never downloaded porn knows a lot about the subject. A third comment by 'B123' asks if an IP address is enough to link a download to an individual. A reply by 'Tawako' says these law suits are to scare people. A comment by 'yes_chate' asks why settlements are offered in the \$2k-\$4k range when they could be getting 60x as much. A reply by 'hedges Your Peak' says if you can easily prove your innocence, you pay nothing. A final comment by 'remygod' says you shouldn't need to prove your innocence; they need to prove your guilt. A reply by 'mikeky' says if by easily you mean paying more in legal fees than what the settlement costs, sure. A final comment by 'redbulence928' says there's pretty much no instance in the legal world of it costing you nothing; it's stressful, time-consuming, and even if you win a case and are awarded legal fees, that entire time you had to pay out of pocket to your lawyers, and not



FRESH
CAPITAL



YOU MUST
REMEMBER
THIS



CAUGHT IN
THE WEBB

Like 1.6k Follow

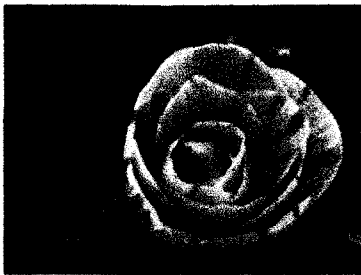
THEY SEE ME TROLLIN'

Accused of Illegally Downloading Porn, Man Demands Public Apology

But he also wants money, because sometimes "sorry" just won't cut it.

By Kelly Faircloth 7/24 11:45am

Twitter 6 Facebook 2 Reddit LinkedIn Email Print



The Google Image results for "porn" are too vile, so here is a "lady flower." (Photo: flickr.com/danseprofane)

Plenty of people have been sued for illegal downloading. But an increasing number of defendants are basically giving plaintiffs the finger, in the form of countersuits. Today TorrentFreak offers up yet another example, that of a put-upon Colorado man who's filed a lengthy countersuit demanding millions in damages and also a public apology in a local newspaper.

Presumably he also faxed the company a handwritten note saying, "And that's what's up."

A bit of background, for those of you

who've never had the misfortune of being caught downloading something illegal: While the RIAA and its big-label ilk have backed off of lawsuits as a tactic for fighting illegal downloading, several porn companies are still using that particular stick. Only rather than dragging the case to trial, companies oh-so-kindly offer their prey a chance to settle for just a few thousand dollars, thereby avoiding becoming "that dude who got sued for downloading *Anal Shuts Vol. XVII*."

Well, Jeff Fantalis wasn't having any of that. He's slapped the company with a 53-page counterclaim, alleging "defamation, the intentional infliction of emotional distress, abuse of process and invasion of privacy." He would like a million dollars in damages for each claim. Go big or go home, we suppose.

In the course of the filing, Mr. Fantalis denies everything in Malibu Media's lawsuit. For starters, tracing illegal downloads to specific IP address is by no means a foolproof method of identifying the actual downloader. He also denies that he has ever seen a pornographic movie in his entire life, which... if you say so, buddy. He even goes far as to suggest that pornography can't even be copyrighted, claiming, according to TorrentFreak, that "explicit porn doesn't fit the basic principle that copyright should promote 'the progress of science' or 'useful arts.'"

But besides the money, Mr. Fantalis would also like "a public retraction and apology in a local newspaper ad, not smaller than a quarter page." He has a few other requirements, as well:

"...[The advertisement] shall specifically retract the claims of the Complaint, acknowledge that Plaintiff wrongfully brought this lawsuit against the Defendant, state that this lawsuit was groundless, acknowledge that the Defendant had not infringed in any manner against the plaintiff and that Defendant is innocent in this matter, and apologize to the Defendant..."

We've reached out to Mr. Fantalis for comment and will update if we hear anything back.

Frankly, we're just amazed anyone anywhere is still bothering to download pornography. You guys know about YouPorn, right?

VOICE ACTIVATED

OneTok Launches Platform Allowing Devs to Easily Integrate Voice Recognition Into Apps

Hawaiians Prepare for Inevitable Larry Ellison Movie 'I Bought an Island'

Dear TV Obsessives, TV Guide's New App Is Actually Pretty Great

Twitter Continues on Its Whirlwind Tour of Alienating Everyone

Raise Your Glass to the Deadpool at 'Startup Funeral' This September

I Have 50 Dollars, 'A Real-Time Social Feed for People Who Have \$50,' Hilariously Satirizes App.net

email address