UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

MALIBU MEDIA, LLC,	:	
	:	Civil Action No. 2012-2078
Plaintiff,	:	
	:	Consolidated from Cases:
vs.	:	2:12-cv-02078-MMB
	:	2:12-cv-02084-MMB
JOHN DOES 1, 6, 13, 14, and 16,	:	5:12-cv-02088-MMB
	:	
Defendants.	:	

PLAINTIFF'S PROPOSED FINDINGS OF FACT

Plaintiff, Malibu Media, LLC, hereby submits the following proposed findings of facts.

I. HOW THE BITTORRENT PROTOCOL WORKS

1. BitTorrent is reciprocal computer network that enables peer-to-peer file sharing.

2. Its popularity stems from its ability to distribute a large file without creating a heavy load on the source computer and network. In short, to reduce the load on the source computer, rather than downloading a file from a single source computer (one computer directly connected to another), the BitTorrent protocol allows users to join a "swarm" of host computers to download and upload from each other simultaneously (one computer connected to numerous computers).

3. A BitTorrent "Client" is a software program that implements the BitTorrent protocol. There are numerous such software programs.

4. A BitTorrent user that wants to upload a new file, known as an "initial seeder," starts by creating a .torrent file using the Client he or she installed onto his or her computer.

5. The Client takes the target computer file and divides it into "pieces."

6. The Client then gives each one of the computer file's pieces a unique alphanumeric identifier known as a Hash Value and records these Hash Values in the .torrent file.

7. The entire .torrent file also has a Hash Value, which at trial was referred to as the Master Hash Value.

8. A Hash Value is like a digital fingerprint for data. Since it is unique, the Master Hash Value identifies only one .torrent file.

9. A file transfer begins when one user accesses the Internet and intentionally makes a digital file of a work available to the public from his or her computer.

10. Other users, who are referred to as 'peers,' then access the Internet and request the file.

11. These users' computers engage each other in a group, referred to as a 'swarm,' and begin downloading and distributing the seed file. Among others, this case involved .mov, .avi and .mp4 files (collectively "Movie Files") which were copies of Plaintiff's copyrighted works. As each peer receives pieces of the Movie Files, that peer makes those pieces available to other peers in the swarm.

12. In order to use BitTorrent, a peer performs six steps.

13. First, a peer installs a BitTorrent client onto his computer.

14. Then he surfs the web to find a .torrent file with the content he wishes to download.

15. Next he clicks on a link to a .torrent file.

16. Then he decides where to save the file on his computer.

17. Then he waits for the download to complete.

18. Finally, after the download is completed, he stops his BitTorrent Client from continuing to distribute pieces of the Movie File. BitTorrent Clients keep uploading pieces until the command is given to stop the infringement.

II. MALIBU MEDIA IS THE VICTIM OF A MASSIVE AMOUNT OF BITTORRENT PIRACY

19. Malibu Media, LLC ("Malibu Media") is owned by Colette Field and her husband Brigham Field.

20. Malibu Media produces its own movies. Malibu Media's niche is the production of high definition movies for adults. Mrs. Field testified that Malibu Media aims to be more artistic than the average adult entertainment website, and that Malibu Media's products are intended to be appealing to men, women and couples.

21. Malibu Media's products are sold through its subscription based website which uses the domain name www.x-art.com.

22. In the lexicon of intellectual property law, a "troll" describes an entity that purchases an intellectual property right for the purpose of licensing it or for the purpose of suing for the infringement of the intellectual property right. Put another way, a troll is not the inventor or author of an intellectual property right. By definition, an intellectual property troll does not use the right for any other purpose but to extract money from third parties through licensing or lawsuits. The word "troll" has a negative connotation.

23. This Court directly asked Mrs. Field if Malibu Media had ever sold its right to enforce its copyrights to a third party. Mrs. Field credibly and unequivocally answered "no."

24. Malibu Media is not a copyright troll.

25. Malibu Media has not sold its copyrights to a copyright troll.

26. Malibu Media is identified as the registrant on each of the United States Copyright Registrations which cover the movies at issue in this lawsuit. Each of these registrations was introduced into evidence at trial through Mrs. Field.

27. Malibu Media's owners worked hard to create their business from scratch.

28. For the first three years, Malibu Media's business had a negative cash flow. During this time, the owners of Malibu Media were investing substantially all of their disposable income into building Malibu Media.

29. Mrs. Field was working two jobs during this period of time and taking money from her paying job and putting it into the business. For the first three years, despite working long hours, the Fields did not take money out of the business.

30. Mrs. Field testified credibly that she has put her heart and soul into Malibu Media, from its inception until the present. She further testified that she works long hours to make the business successful.

31. For the first couple of years of its existence, Malibu Media had a production budget of between $150,000 and $200,000 a year.

32. It now spends over $2,000,000 a year to produce its movies.

33. Its subscriber base has grown from about 500 in year one to approximately 50,000 now.

34. It costs a substantial amount of money to operate Malibu Media's business. Malibu Media must pay models, for servers, for website maintenance, for bandwidth, for locations, among myriad other things.

35. More people are watching Malibu Media's movies in 2013 than were watching them in 2012.

36. Malibu Media's subscription base has not increased over the last several years, however, because people are downloading its movies from free via the BitTorrent Protocol.

37. Malibu Media subscribers routinely ask Malibu Media why they should pay a subscription fee when they can get its movies for free through BitTorrent.

38. Since it has real costs, Malibu Media cannot compete with free copies of its movies.

39. Twice in 2013, unknown third parties hacked into Malibu Media's servers and put its movies onto BitTorrent prior to the time that these movies were released onto Malibu Media's website. These incidents cost Malibu Media thousands of dollars in lost subscription revenue.

40. Malibu Media now encrypts their movies prior to releasing them.

41. But this does not stop the infringement from occurring once the movie has been unencrypted and then viewed. All it does is stop the theft of its movies prior to release.

42. As a consequence, Malibu Media spends approximately $15,000 a month on enhanced security features.

43. Many of Malibu Media's subscribers have complained that they can download its movies faster from BitTorrent than they can from its website.

44. Consequently, Malibu Media started spending approximately $20,000 more a month this year to make its downloading speed faster than that which can be achieved through BitTorrent.

45. In May 2013, over 80,000 people illegally downloaded Malibu Media's movies in the United States through BitTorrent. This was a typical month.

46. In May 2013, over 300,000 people illegally downloaded Malibu Media's movies in the fifteen countries that IPP, Ltd., Malibu Media's investigator tracks infringement for Malibu Media. This was a typical month.

47. While the exact amount would be speculative, the Court has no doubt that BitTorrent infringement costs Malibu Media millions of dollars each year in direct costs and lost subscription sales.

48. Mrs. Field testified credibly that Malibu Media would be reinvesting a substantial amount of the money it loses from BitTorrent infringement back into its business. Specifically, this money would be spent on more content and improving its products and services.

49. BitTorrent infringement is depriving Malibu Media's paying subscribers of the benefit of enjoying more of Malibu Media's content because that content is not being produced.

50. Malibu Media sends 1000s of DMCA notices each month aimed at stopping the infringement of its copyrights through BitTorrent.

51. Many torrent websites, including The Pirate Bay, do not respect U.S. Copyright laws and intentionally situate themselves in countries outside the reach of copyright laws. Mrs. Field testified credibly that she believes that this makes stopping the problem of BitTorrent piracy by suing the websites prohibitively expensive and unlikely to succeed.

52. Many BitTorrent Clients are also located in countries outside the reach of copyright laws. BitTorrent software can be used for legitimate non-infringing means. Mrs. Field testified credibly that she believes that this makes stopping the problem of BitTorrent piracy by suing the torrent websites prohibitively expensive and unlikely to succeed.

53. BitTorrent, Inc. merely writes and improves the protocol, in other words, the computer code used to operate BitTorrent. It then licenses this code to BitTorrent Clients. The

BitTorrent Protocol can be used for legitimate non-infringing purposes. Mrs. Field testified credibly that she believes suing BitTorrent, Inc. would be prohibitively expensive for Malibu Media.

54. There are over 10 million .torrent files available to be downloaded by using the BitTorrent protocol.

55. Approximately, 100 million people use BitTorrent worldwide on an average day.

56. Each .torrent file represents a movie, song, software program, book, or some other type of media, program or computer file. Almost all major motion pictures are available for free on BitTorrent.

57. BitTorrent piracy causes not only Malibu Media substantial actual damages but it also causes substantial damage to mainstream movie studios, software companies, songwriters and authors.

58. Malibu Media has the right to file these types of cases in Philadelphia and across the country and should not be discriminated against on the basis that it produces adult content or because it has filed numerous similar cases in the past.

III. THE DEFENDANT'S IP ADDRESS WAS CORRELATED CORRECTLY TO THE INFRINGEMENT

59. Malibu Media hired IPP, Ltd. ("IPP") to identify the IP addresses being used to download and distribute Malibu Media's movies through BitTorrent.

60. Michael Patzer testified about how IPP's software works.

61. The IP detection process begins when IPP's clients, here Malibu Media, provide IPP with the names of their copyrighted works. IPP's software then does a lexical scan of torrent websites for possible matches.

62. Once a possible match is found, IPP downloads the computer file associated with the .torrent file and starts logging data from possible infringers.

63. IPP's software establishes a successful TCP/IP connection. It also establishes a successful BitTorrent handshake. Its software then asks the infringing peer for data. The infringing peer then sends a piece of the data. For each Defendant many such transactions are logged. The Hash Values of the .torrent file and the Hash Values of the pieces of data are checked against the index in a .torrent file to ensure that it is a part of a Movie File that is a copy of Malibu Media's work.

64. IPP's software does not, and is not capable of distributing pieces of Movie Files back into a BitTorrent swarm.

65. IPP records the transaction with the infringer on a WORM tape drive which stands for "write-once-read-many". Because you can only write on the tape drive once, the drive cannot be altered. The transactions on the worm tape drive receive a time-stamp from the German government to ensure that the data was written to the WORM drive on the same day it was recorded.

66. Each BitTorrent transaction in which pieces of a file are delivered lasts at least two seconds before and two seconds after the data is delivered to IPP.

67. The transactions are saved in a PCAP file which stands for "Packet Capture". The type of packet the PCAP file captures is a data packet. IPP uses a program called a "TCP-Dump" to create PCAPs and record all of the network transactions that its server receives and transmits. This process is akin to a video camera recording all the ins-and-outs of transactions to and from IPP's servers.

68. Based upon the foregoing, and Patrick Paige's testimony summarized below, this Court finds that IPP's software accurately and reliably identifies the IP Addresses of those people distributing pieces of data in a BitTorrent swarm.

B. Testimony of Tobias Feiser

69. Tobias Feiser, IPP's employee, verifies that the movies downloaded on BitTorrent belong to the Plaintiff. He views the copies obtained through BitTorrent and compares them with the original movies owned by Plaintiff.

70. At least one other IPP employee also verifies that the movies obtained through BitTorrent match the original.

71. Exhibits were introduced containing the official movies and the copies of the movies created through BitTorrent.

72. After verifying that the movies transmitted through BitTorrent match the movies owned by Malibu Media, Mr. Feiser sends the infringement data to Plaintiff's law firm.

73. Before filing these lawsuits, Plaintiff's law firm sent Mr. Feiser the exhibits attached to the Complaint. Mr. Feiser uploaded the data on the litigation exhibits into IPP's software. IPP's software then verified that the litigation exhibits were correct by displaying a green light on Mr. Feiser's computer. In situations where the information on a litigation exhibit is not correct, Mr. Feiser's computer displays a red light. For all the exhibits in this case, Mr. Feiser's computer displayed a green light.

74. Based upon Mr. Patzer's testimony, Mr. Feiser's testimony, and Mr. Paige's test of IPP, Ltd.'s software, described below, it is clear that IPP, Ltd.'s IP Address detection is able to accurately and reliably identify the IP Address of a peer in a BitTorrent swarm.

75. IPP's evidence established that John Doe 1's IP Address was used to infringe four (4) movies the copyrights to which were registered by Malibu Media with the United States Copyright Office ("Registered Movies), John Doe 13's IP Address was used to infringe thirty-five (35) Registered Movies, and Bryan White's IP Address was used to infringe five (5) Registered Movies.

C. Internet Service Provider ("ISP") Correlation

76. After this Court granted Malibu Media leave to subpoena Comcast and Verizon to obtain the identities of the John Doe defendants, Malibu Media's law firm sent the ISPs a subpoena with the corresponding exhibits from its Complaint to correlate the IP address to an individual subscriber who owned and controlled the IP address at the time of infringement.

77. The parties stipulated that the correlations done by the ISPs were accurate and reliable. Plaintiff also read into evidence testimony from Colin Padgett who testified as the corporate representative for Comcast during a discovery deposition. Mr. Padgett testified that Comcast was "absolutely certain" that the correlation for John Doe 1 was done correctly.

78. Based upon the foregoing, I find that Verizon and Comcast's correlation techniques are accurate and reliable and that they worked in this case.

D. Testimony of Patrick Paige

(I) WiFi Hacking

79. The Court finds Patrick Paige is qualified as an expert in computer forensics and is competent to give opinion testimony. Patrick Paige testified he has a long history as a computer forensic analyst with law enforcement, worked for a leading manufacturer of computer forensic software, has received numerous awards from the U.S. Government in association with his cases involving child pornography, has taught computer forensic courses to other law

enforcement officers, and has been admitted as expert in numerous other federal and state court cases throughout the country.

80. Patrick Paige testified that he had personally been involved in investigating computers seized from homes following the issuance of search warrants.

81. Significantly, just as in this case, the search warrants were issued after law enforcement officers established a successful TCP/IP connection with a computer.

82. Only once in connection with approximately two hundred search warrants did Mr. Paige fail to find the illegal content on a computer seized from the home identified in the search warrant.

83. In that one instance, the transmission came from the house behind the subscriber's house. And, the subscriber had an open WiFi. In other words, the WiFi was not password protected. Further, the suspect was wanted for child pornography. The Court takes judicial notice that a child pornographer has a greater incentive to hack WiFi routers than BitTorrent infringers.

84. Accordingly, out of approximately two hundred search warrants wherein Mr. Paige was able to use the power of the state to seize evidence, he did not run into one instance of WiFi hacking.

85. Bryan White asserted a WiFi hacking defense in bad faith.

86. The Court takes judicial notice that many people in Philadelphia and across the country have asserted WiFi hacking as a defense in cases involving BitTorrent infringement. Without corroborating evidence, the Court finds the defense of WiFi hacking is highly suspect.

87. The Court further advises Doe Defendants in Philadelphia and across the country that perjury will not be tolerated in Federal Courts. Doe Defendants and their counsel should also be advised that Fed.R.Civ.P. 11(b)(3) applies to the defense of WiFi hacking.

(II) Test of IPP's Software

88. By using four uncopyrighted works in the public domain, Mr. Paige recreated the process used by Doe Defendants to distribute Plaintiff's copyrighted works. He used four test servers each of which had a different IP Address. IPP was able to identify accurately every video, record his IP and send him the PCAPs of each transaction. Mr. Paige was running a program called Wireshark on his test servers. Like TCP Dump, used by IPP, Ltd., Wireshark creates PCAPs. Again, PCAPs are analogous to a video recording of all of the transmissions in and out of a computer. IPP's PCAPs matched Mr. Paige's PCAPs. This could not have happened if IPP was not actually connected to Mr. Paige's test servers. IPP accurately identified the IP Addresses of Mr. Paige's test servers. If a party subpoenaed the identity of the owner of the IP Addresses of Mr. Paige's test servers from the ISPs used by Mr. Paige, that person would have learned Mr. Paige's identity.

89. Mr. Paige's testimony further establishes that IPP, Ltd.'s IP Address detection process is accurate and reliable.

IV. JOHN DOE 1 INFRINGED PLAINTIFF'S COPYRIGHTS

90. John Doe 1 initially denied committing the infringement and even denied it under oath during a deposition.

91. John Doe 1's Internet service was password protected.

92. John Doe 1 knew about BitTorrent prior to the infringement.

93. John Doe 1 admitted in a declaration that he intentionally infringed upon Malibu Media's works.

94. John Doe 1 is out of the Country and waived his right to be at this trial.

95. I find that John Doe 1 is liable for intentionally infringing Malibu Media, LLC's copyright works as alleged in the pleadings filed in this matter.

V. JOHN DOE 13 INFRINGED PLAINTIFF'S COPYRIGHTS

96. John Doe 13 installed a BitTorrent Client onto his computer.

97. John Doe 13 intentionally downloaded Plaintiff's movies with the full knowledge he was infringing Plaintiff's copyrights. He understood this meant he was distributing Plaintiff's movies. Further, he testified that he knew that using BitTorrent to download and distribute copyrighted content violates U.S. Copyright laws and that his infringement was intentional.

98. Based on his testimony, I find that John Doe 13 is liable for intentionally infringing Malibu Media, LLC's copyrighted works as alleged in the pleadings filed in this matter.

99. At no point at any time during the course of litigation did John Doe 13 deny he committed the infringement, even when he filed his motion to quash.

VI. BRYAN WHITE INFRINGED PLAINTIFF'S COPYRIGHTS

100. Mr. White's computers indicate that substantial amounts of data were permanently erased from them.

101. Mr. White denied under oath while being directly questioned by the Court that he did not install Windows onto his computer on November 11, 2012, three days after Plaintiff served Mr. White with their request for production of documents which included a copy of his hard drive.

102. Patrick Paige called Microsoft and after providing it with Mr. White's product license key, asked when it was last activated. Microsoft's records indicate that it was last activated on November 11, 2012.

103. The Court appointed expert, Louis Cinquanto, testified that Windows was installed on his computer on November 11, 2012.

104. Based on the testimony of Mr. Paige, Mr. Cinquanto, and Microsoft's records, I find that Mr. White's testimony was not credible.

105. I also find that Mr. White destroyed material evidence and then tried to cover up his destruction of evidence.

106. Just before jury selection was to begin, Mr. White agreed to admit that he was liable for infringing Plaintiff's copyrighted movies. Through his counsel, he did so at trial.

107. Based upon the foregoing, the Court finds that Mr. White infringed Plaintiff's copyrights alleged in the Amended Complaint and is liable to Plaintiff for copyright infringement.

Dated: June 12, 2013.

Respectfully submitted,

LIPSCOMB, EISENBERG & BAKER, PL

By: /s/ *M. Keith Lipscomb*
M. Keith Lipscomb (Fla. Bar. No.429554)
klipscomb@lebfirm.com
LIPSCOMB, EISENBERG & BAKER, PL
2 South Biscayne Blvd.
Penthouse 3800
Miami, FL 33131
Telephone: (786) 431-2228
Facsimile: (786) 431-2229
ATTORNEYS FOR PLAINTIFF

and,

Christopher P. Fiore, Esquire
Aman M. Barber, III, Esquire
425 Main Street, Suite 200
Harleysville, PA 19438
Tel: (215) 256-0205
Fax: (215) 256-9205
Email: cfiore@fiorebarber.com
ATTORNEYS FOR PLAINTIFF

CERTIFICATE OF SERVICE

I hereby certify that on June 12, 2013, I electronically filed the foregoing document with the Clerk of the Court using CM/ECF and that service was perfected on all counsel of record and interested parties through this system.

By: /s/ *M. Keith Lipscomb*