

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MASSACHUSETTS**

LIBERTY MEDIA HOLDINGS, LLC,

Plaintiff,

vs.

SWARM SHARING HASH FILE  
AE340D0560129AFEE8D78CE07F2394C7B5B  
C9C05; AND DOES 1 through 38,

Defendants.

Civil Action No. 11-cv-10802-MBB

**DECLARATION OF MALTE DINKELA**

I, Malte Dinkela, declare:

1. I am the Vice President of Excubitor USA, Inc., a company incorporated in Nevada with its principal address at 4550 West Oakey Blvd. #111H, Las Vegas, NV 89102. Excubitor is a provider of online antipiracy services for the motion picture industry. Before my employment with Excubitor, I held various positions at companies that developed software technologies. I have approximately ten years of experience related to digital media and computer technology.

2. I submit this declaration in support of Liberty Media Holdings, LLC's Complaint for Copyright Infringement and Plaintiffs Motion for Leave to Take Early Discovery. This declaration is based on my personal knowledge, and if called upon to do so, I would be prepared to testify as to its truth and accuracy.

3. At Excubitor, I am the head of the department that carries out evidence collection and provides litigation support services. I work closely with our research team to create credible processes to scan for, detect, and document copyright infringement conducted over the internet.

4. The Internet is a vast collection of interconnected computers and computer networks that communicate with each other. It allows hundreds of millions of people around the world to freely and easily exchange ideas and information. Unfortunately, the Internet also has afforded opportunities for wide scale infringement of copyrighted motion pictures. Once a motion picture has been transformed into an unsecured digital format, it can be further copied and distributed an unlimited number of times over the Internet, without significant degradation in picture or sound quality.

5. To copy and distribute copyrighted motion pictures over the Internet, many individuals use online media distribution systems or so-called “peer-to-peer” (“P2P”) networks. P2P networks, at least in their most common form, are computer systems that enable Internet users to (1) make files (including motion pictures) stored on each user’s computer available for copying by other users or peers; (2) search for files stored on other users’ computers; and (3) transfer exact copies of files from one computer to another via the Internet.

6. The plaintiff in this action, Liberty Media Holdings, LLC (“Plaintiff”) is a producer and distributor of motion pictures. On behalf of Plaintiff, we engaged in a specific process utilizing Excubitor’s specially designed software technology to identify direct infringers of Plaintiff’s copyrighted materials over P2P networks. Plaintiff owns the copyright and the exclusive distribution and licensing rights for the motion picture, “Down on the Farm” (the “Motion Picture”). Excubitor has documented evidence of the unauthorized reproduction and distribution of the Motion Picture within the United States of America, including the Commonwealth of Massachusetts.

### **EXPLANATION OF THE BITTORRENT PROTOCOL**

7. Excubitor has licensed a proprietary technology that provides an effective means of detecting the unauthorized distribution of movies and other content over P2P networks. Excubitor's technology enables it to detect and monitor the transfer and distribution of files amongst the P2P networks.

8. Excubitor's present investigation for Plaintiff focuses on the unauthorized distribution of the Motion Picture over the BitTorrent P2P protocol. BitTorrent is a peer-to-peer file sharing protocol used for distributing and sharing data on the Internet, including files containing digital versions of motion pictures. Rather than downloading a file from a single source, the BitTorrent protocol allows users to join a "swarm," or group of hosts to download and upload from each other simultaneously. The process works as follows:

9. First, users download a torrent file onto their computer. These torrent files do not contain audio or visual media, but instruct the user's BitTorrent client where to go and how to obtain the desired content. The torrent file contains a unique hash code known as the SHA-1 hash — which is a unique identifier generated by a mathematical algorithm developed by the National Security Agency. This torrent file also contains a "roadmap" to the Internet Protocol ("IP") addresses of other users who are sharing the media file identified by the unique hash code, as well as specifics about the media file. The media file could be any large file, including a digital motion picture or music file.

10. Because BitTorrent client software generally lacks the ability to search for torrents, end-users use search engines or other websites that contain indices of torrent files to locate torrent files being made available by other BitTorrent users.

11. Second, the user opens the torrent file with a BitTorrent program, also known as a BitTorrent “client” application, which is capable of reading the roadmap encoded in the torrent file. This client program, after reading the roadmap, connects “uploaders” of the file (i.e., individuals that are distributing the content) with “downloaders” of the file (i.e., individuals that are copying the content). During this process, the BitTorrent client reaches out to one or more “trackers” that are identified on the roadmap. A tracker is an Internet server application that records the IP addresses associated with users who are currently sharing any number of media files identified by their unique hash values and then directs a BitTorrent user’s computer to other users who have the particular file each user is seeking to download.

12. Each IP address identified by the tracker is an uploading user who is currently running a BitTorrent client on his or her computer and who is currently offering the desired motion picture file for download. The downloading user’s BitTorrent software then begins downloading the motion picture file without any further effort from the user, by communicating with the BitTorrent client programs running on the uploading users’ computers.

13. The life cycle of a file shared using BitTorrent begins with just one individual — the initial propagator, sometimes called a “seed” user or “seeder.” The initial propagator intentionally elects to share a file with a torrent swarm. The original file, in this case, contains Plaintiff’s entire copyrighted Motion Picture.

14. Other members of the swarm connect to the seed to download the file, wherein the download creates an exact digital copy of Plaintiff’s copyrighted Motion Picture on the downloaders’ computers. As additional thieves request the same file, each additional thief joins the collective swarm, and each new thief receives pieces of the file from each other thief in the swarm who has already downloaded any part of the file. Eventually, once the initial propagator

has distributed each piece of the file to at least one other thief, so that together the pieces downloaded by members of the swarm comprises the whole Motion Picture when reassembled, the initial propagator may leave the swarm, and the remaining thieves can still obtain a full copy of the Motion Picture by exchanging the pieces of the Motion Picture that each one has.

15. Files downloaded in this method are received in hundreds or even thousands of individual pieces. Each piece may be contributed from a different member of the swarm. Moreover, each piece that is downloaded is immediately thereafter made available for distribution to other users seeking the same complete file. Thus, the effect of this technology effectively makes every downloader of the content also an uploader. This means that every user who has a copy of the infringing material in a swarm may also be a source for later downloaders of that material.

16. In the BitTorrent world, there is honor among thieves. Those who merely download files, without publishing and sharing files, are derisively called “leechers.” Being a leecher is not only a negative due to the pejorative terminology, but leechers are also punished by the torrent swarm. The BitTorrent protocol stalls the downloads of leechers in an effort to preserve network speed for the more prolific copyright infringers. Thus, the sharing of files as users receive them is inherent in BitTorrent’s use.

17. This distributed nature of BitTorrent leads to a rapid viral sharing of a file throughout the collective peer users. As more peers join the collective swarm, the frequency of successful downloads also increases. Because of the nature of the BitTorrent protocol, any seed peer that has downloaded a file prior to the time that a subsequent peer downloads the same file is automatically a source for the subsequent peer, so long as that first peer is online at the time the subsequent peer requests the file from the swarm. Because of the nature of the collective

swarm, every infringer is — and by necessity all infringers together are — simultaneously both stealing the Plaintiff's copyrighted material and redistributing it.

### INVESTIGATIVE METHODOLOGY

18. I am responsible for identifying online piracy of motion pictures for Excubitor, including gathering evidence of online piracy to support Plaintiff's copyright protection enforcement efforts.

19. As the first step in identifying potential infringers of the Motion Picture, Excubitor searched websites indexing torrent files for a file labeled with the name of the Motion Picture. Once a suspicious torrent file was identified, Excubitor downloaded the associated file from the BitTorrent network, viewed it, and confirmed that it was in fact an unauthorized copy of the Motion Picture.

20. Once we confirmed that the torrent file referenced an infringing copy of the Motion Picture, we then extracted the unique hash code assigned to the file. The hash code associated with the particular copy of the Motion Picture at issue in this litigation is AE340D0560129AFEE8D78CE07F2394C7B5BC9C05 (the "AE3 Hash").

21. Excubitor's software would then monitor the swarm associated with downloading and distributing the AE3 Hash. Excubitor would investigate each peer connected with the AE3 Hash by downloading a portion of the file from the peer's computer. This download confirmed that the peer was actively distributing the file. The evidence of this download is then saved and documented and could be introduced into evidence as necessary.

22. From the downloaded file, we obtain the Internet Protocol ("IP") address of a user offering the file for download. Although users' IP addresses are not automatically displayed on

the P2P networks, any user's IP address is readily identifiable from the packets of data being exchanged.

23. We also collected other publicly available information that is designed to help Plaintiff identify the infringer. Among other things, we recorded and documented (a) the time and date at which the file or a part of the file was distributed by the user; (b) the IP address assigned to each user at the time of infringement; and, in some cases, (c) the video file's metadata (digital data about the file), such as title and file size. We then created evidence logs for each user and stored all this information in a database.

24. As part of my responsibilities at Excubitor, I have also been designated to confirm that the digital audiovisual files downloaded by Excubitor are actual copies of Plaintiff's Motion Picture. Excubitor (and accordingly, Plaintiff) does not rely solely on the labels and metadata attached to the files themselves, but also confirms the copying through a visual comparison between the downloaded file and the Motion Picture.

25. I have watched the Motion Picture. The downloaded files have been carefully reviewed and compared by a visual comparison with the original Motion Picture. I confirmed that they contain a substantial portion of the Motion Picture identified in the Complaint.

26. As of January 31, 2011, Excubitor identified at least thirty eight (38) unique IP addresses traceable to the Commonwealth of Massachusetts that were engaged in the unauthorized downloading and distribution of the AE3 Hash. A summary of the identified IP address, along with other information Excubitor was able to obtain, is attached hereto as Exhibit A.

27. Plaintiff's Motion Picture continues to be made available for unlawful transfer and distribution using the BitTorrent network. Liberty Media and Excubitor continue to monitor such unlawful distribution and transfer of Plaintiff's motion pictures.

**EXPIDITED DISCOVERY IS NEEDED**

28. Obtaining the identity of copyright infringers on an expedited basis is critical to prosecution of this action and stopping the continued infringement of the Motion Picture. Plaintiff does not have Defendants' names, addresses, e-mail addresses, or any other way to identify or locate Defendants, other than the unique IP address assigned to each Defendant by his/her internet Service Provider on the date and at the time of the Defendant's infringing activity.

29. An IP address is a unique numerical identifier that is automatically assigned to a user by its Internet Service Provider ("ISP") each time a user logs onto the network. Each time a subscriber logs on, he or she may be assigned a different IP address unless the user obtains from his/her ISP a static IP address. ISPs are assigned certain blocks or ranges of IP addresses.

30. An infringer's IP address is significant because it is a unique identifier that, along with the date and time of infringement, specifically identifies a particular computer using the Internet. However, the IP address does not enable us to ascertain with certainty the exact physical location of the computer or to determine the infringer's identity. It only enables us to trace the infringer's access to the Internet to a particular Internet Service Provider ("ISP") and, in most instances, to a general geographic area.

31. Here, the IP addresses Excubitor identified enable us to determine which ISP was used by each infringer to gain access to the Internet. Publicly available databases located on the Internet list the IP address ranges assigned to various ISPs. We determined that the Doe




Defendants here were using those ISPs listed in Exhibit A to gain access to the Internet and distribute and make available for distribution and copying the Motion Picture.

32. ISPs keep track of the IP addresses assigned to its subscribers at any given moment and retain such “user logs” for a limited amount of time. These user logs provide the most accurate means to connect an infringer’s identity to its infringing activity. Further, ISPs have different policies pertaining to the length of time they preserve their user logs. Despite requests to preserve the information, some ISPs keep the session data of their subscribers’ activities for only limited periods of time — sometimes as little as weeks or even days — before erasing the data they contain.

33. Once ISP’s are provided with the IP address, plus the date and time of the infringing activity, the ISPs can quickly and easily use their respective subscriber logs to identify the name and address of the ISP subscriber who was assigned that IP address at that date and time.

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

Executed on <sup>05/09/2011</sup> \_\_\_\_\_, at my offices in Bochum, Germany.

  
\_\_\_\_\_  
MALTE DINKELA

**EXHIBIT A****IP Addresses of John Does Identified as Sharing Infringing Copies of Down on the Farm  
(Hash Code: AE340D0560129AFEE8D78CE07F2394C7B5BC9C05)**

<b>IP Address</b>	<b>Hit Date (UTC)</b>	<b>ISP</b>	<b>Estimated City</b>
71.233.168.113	15.11.2010 16:01:38	Comcast Cable	Lowell
66.30.115.104	15.11.2010 19:55:10	Comcast Cable	Cambridge
24.147.176.193	16.11.2010 02:39:24	Comcast Cable	Boston
76.119.104.125	16.11.2010 04:13:47	Comcast Cable	Northampton
76.19.23.251	16.11.2010 06:46:32	Comcast Cable	Boston
71.233.69.203	16.11.2010 23:32:02	Comcast Cable	Bellingham
71.192.242.221	17.11.2010 05:03:22	Comcast Cable	Roslindale
98.216.106.88	17.11.2010 06:36:09	Comcast Cable	Cambridge
68.112.244.132	17.11.2010 07:06:55	Charter Communications	Worcester
24.91.60.179	17.11.2010 21:15:42	Comcast Cable	Marlborough
98.216.154.230	17.11.2010 21:22:11	Comcast Cable	Brookline
216.15.127.56	18.11.2010 16:32:22	RCN Corporation	Allston
75.69.46.3	21.11.2010 01:01:28	Comcast Cable	Whately
24.2.207.9	21.11.2010 12:58:22	Comcast Cable	Beverly
97.80.121.93	21.11.2010 18:48:09	Charter Communications	Chicopee
71.192.115.67	22.11.2010 03:37:24	Comcast Cable	Woburn
24.62.198.237	23.11.2010 05:49:41	Comcast Cable	Marion
71.192.142.223	23.11.2010 19:05:31	Comcast Cable	Springfield
24.218.109.54	24.11.2010 07:31:48	Comcast Cable	Boston

<b>IP Address</b>	<b>Hit Date (UTC)</b>	<b>ISP</b>	<b>Estimated City</b>
173.76.111.98	25.11.2010 03:19:14	Verizon Internet Services	Marlborough
24.60.16.41	25.11.2010 15:49:25	Comcast Cable	Chestnut Hill
24.62.137.164	27.11.2010 03:04:20	Comcast Cable	Lowell
24.218.205.41	27.11.2010 22:04:23	Comcast Cable	Boston
71.233.245.203	28.11.2010 01:21:36	Comcast Cable	Medford
76.118.182.249	28.11.2010 05:48:05	Comcast Cable	Cambridge
67.186.133.215	01.12.2010 16:35:26	Comcast Cable	Cambridge
76.19.22.236	02.12.2010 05:04:39	Comcast Cable	Boston
72.93.168.241	03.12.2010 02:51:59	Verizon Internet Services	Brookline
98.216.97.159	03.12.2010 09:24:56	Comcast Cable	Medford
72.93.173.3	04.12.2010 05:28:22	Verizon Internet Services	Cambridge
24.61.203.200	06.12.2010 07:43:31	Comcast Cable	Lowell
24.61.83.19	07.12.2010 07:38:19	Comcast Cable	Boston
71.88.111.96	07.12.2010 09:08:37	Charter Communications	Worcester
76.118.202.126	08.12.2010 00:25:42	Comcast Cable	Attleboro
98.217.178.128	09.12.2010 02:03:42	Comcast Cable	Boston
65.96.125.104	29.01.2011 05:39:22	Comcast Cable	Boston
209.6.49.239	30.01.2011 14:09:39	RCN Corporation	Somerville
71.232.55.106	31.01.2011 03:11:08	Comcast Cable	Boston