

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

EXHIBIT A

1 Brett L. Gibbs, Esq. (SBN 251000)
Steele Hansmeier PLLC.
2 38 Miller Avenue, #263
Mill Valley, CA 94941
3 415-325-5900
blgibbs@wefightpiracy.com

4 *Attorney for Plaintiff*
5

6
7 IN THE UNITED STATES DISTRICT COURT FOR THE
8
9 NORTHERN DISTRICT OF CALIFORNIA
10
11 OAKLAND DIVISION

11 HARD DRIVE PRODUCTIONS, INC.,)
12)
13 Plaintiff,)
14 v.)
15 DOES 1-118,)
16 Defendants.)

No. C-11-01567 LB

**DECLARATION OF
PETER HANSMEIER IN SUPPORT OF
EX PARTE APPLICATION FOR LEAVE
TO TAKE EXPEDITED DISCOVERY**

17
18 **DECLARATION OF PETER HANSMEIER IN SUPPORT OF EX PARTE APPLICATION
FOR LEAVE TO TAKE EXPEDITED DISCOVERY**

19 I, Peter Hansmeier, declare under penalty of perjury as true and correct that:

20
21 1. I am a technician at Media Copyright Group, LLC (“MCG”). On behalf of its clients,
22 MCG monitors and documents Internet-based piracy of our clients’ copyrighted creative works. I
23 submit this declaration in support of Plaintiff’s *Ex Parte* Application for Leave to Take Expedited
24 Discovery.

25 2. The Plaintiff in this action is an exclusive licensee of the right to distribute and
26 reproduce certain copyrighted creative works via the BitTorrent protocol. We have been engaged to
27 collect and document evidence of the unauthorized reproduction and distribution of the copyrighted
28

1 7. Modern peer-to-peer file transfer protocols substantially avoid these problems by
2 allowing each data-seeking user to both upload to and download from other data-seeking users
3 without the material assistance of a robust central server. In contrast to traditional file transfer
4 protocols, modern peer-to-peer protocols actually work *better* when large numbers of users request
5 data simultaneously because as the number of users seeking a file grows, so too does the number of
6 users from which to download the file. Moreover, a distributed web of users is far more difficult to
7 shut down than a central server.
8

9 8. The most popular and peer-to-peer file transfer protocol is the BitTorrent protocol.
10 Studies have estimated that the BitTorrent protocol accounts for up to 70% of all peer-to-peer traffic
11 and as much as 50% of all Internet traffic in some parts of the world. In BitTorrent vernacular,
12 individual downloaders of a file are called peers. The aggregate group of peers involved in
13 downloading a particular file is called a swarm. A server that stores a list of peers in a swarm is
14 called a tracker. A computer program that implements the BitTorrent protocol is called a BitTorrent
15 client.
16

17 9. The sharing of a file via the BitTorrent protocol operates as follows. First, a person
18 who possesses a complete digital reproduction of a given file intentionally elects to share the file
19 with other Internet users. That complete file is called a “seed.” The initial “seeder” creates a small
20 “torrent” file that contains instructions for how to find the seed. The seeder uploads the torrent file
21 to one or more of the many torrent indexing sites. As Internet users come across the torrent file, they
22 intentionally elect to load the torrent files in their BitTorrent client, which uses the instructions
23 contained in the torrent file to locate the seed. These users now are peers in a swarm with respect to
24 that digital reproduction. The BitTorrent protocol dictates that each peer download a random portion
25 of the file (a “piece”) from the seed. After a peer has downloaded its first piece, it then shares that
26 piece and subsequent pieces with other peers in the swarm. The effect of this protocol is that each
27
28

1 peer is both a downloader and uploader of an illegally-transferred file. As more peers join the
2 swarm, the rate of data transfer typically increases because the odds of connecting to another peer
3 improve.

4 10. In observing the swarms that were formed to distribute the copyrighted content
5 subject to Plaintiff's exclusive license, I observed swarms that were hundreds of users large that
6 contained peers from states across the United States as well as many countries around the world. The
7 BitTorrent protocol is particularly well suited to transferring large files, such as the audiovisual
8 works produced by Plaintiff, as it allows even small computers with low bandwidth to be capable of
9 participating in large data transfers across a peer-to-peer network.
10

11 11. Where, as here, a content owner such as Plaintiff has not authorized this uncontrolled
12 mass-reproduction and distribution of its content via the BitTorrent protocol, I believe that the
13 copying and distribution of its content violates copyright laws. Because BitTorrent is a distributed
14 protocol, there is no central server that can be targeted for purposes of stemming the tide of piracy. I
15 believe that seeking recourse against individual content pirates is likely to be the most effective
16 means of addressing BitTorrent-based content piracy.
17

18 **Identification of the Doe Defendants**

19 12. In order to assist Plaintiff in identifying instances of copyright infringement on
20 BitTorrent-based peer-to-peer networks, MCG used sophisticated and proprietary peer-to-peer
21 network forensic software to perform exhaustive real time monitoring of BitTorrent-based swarms
22 involved in distributing the copyrighted creative works relevant to Plaintiff's action. MCG's
23 proprietary software is effective in capturing granular-level data about the activity of peers in a
24 swarm and their infringing conduct and MCG's processes are designed to ensure that information
25 gathered about each Doe Defendant is accurate.
26
27
28

1 13. The first step in the infringer-identification process is to locate swarms where peers
2 are distributing the copyrighted creative works. I accomplished this step by using a variety of
3 techniques to locate torrent files sharing the names of copyrighted creative works subject to
4 Plaintiff's exclusive license. Such files are commonly located on torrent indexing sites, but can also
5 be found on Internet file-sharing forums and areas where users congregate. Because a torrent file
6 only contains directions about where to find the swarm associated with a particular item of digital
7 content, the next step is to locate the swarm.

9 14. The most common means of locating a swarm is to connect to a BitTorrent tracker,
10 which is a server that contains an updated list of peers in a swarm. A typical torrent file contains a
11 list of multiple trackers associated with the underlying file. Other means of locating a swarm
12 include using Distributed Hash Tables, which allow each peer to serve as a "mini-tracker" and Peer
13 Exchange, which allows peers to share data about other peers in the swarm without the use of a
14 tracker. I used all three methods to locate swarms associated with Plaintiff's exclusive license.

16 15. After locating a swarm, I used MCG's proprietary forensic software to conduct an
17 exhaustive real time "fingerprint" of the swarm. In doing so, I collected data on the peers in the
18 swarm, including what activities each peer was engaging in and other important data such as the date
19 and time that each Defendant was observed by the software as engaging in infringing activity and
20 each Defendant's Internet protocol ("IP") address at that date and time. Although I was able to
21 observe Defendants' infringing activity through forensic software, this system does not allow me to
22 access Defendants' computers to obtain identifying information other than an IP address. Nor does
23 this software allow me to upload a file onto Defendant's computer or otherwise to communicate with
24 it.
25

26 16. An IP address is a unique number that is assigned to Internet users by an Internet
27 service provider at a given date and time. There are two types of IP addresses: dynamic and static.
28

1 A static IP address is an IP address that will be associated with a particular user as long as that user
2 is a customer of a given Internet service provider. A dynamic IP address is an IP address that will
3 change from time-to-time.

4 17. Most consumer customers of Internet service providers are assigned a dynamic IP
5 address. The reason for this is that an Internet Service provider can get by with a smaller overall
6 pool of IP addresses if it simply assigns the next available IP address at a given time to a customer
7 who wishes to connect to the Internet versus allocating a permanent and unique IP address to each
8 of its users. Internet service providers keep logs of IP addresses, but the length of time they keep the
9 logs can be as short as days, making expedited discovery of the identities associated with those IP
10 addresses critically important in the instant action, particularly since nearly all of the Defendants I
11 observed appeared to be associated with dynamic IP addresses.

12 18. After recording granular level data about every peer in the swarm, the next step is to
13 carefully and thoroughly review the data produced by MCG's proprietary forensic software to
14 determine what peers were actually involved in illegally reproducing and distributing our client's
15 copyrighted creative works. We then trace each offending IP address to specific ISPs. I performed
16 this work with respect to the copyrighted creative content subject to Plaintiff's exclusive license.

17 19. When a verified peer was located who was making files subject to Plaintiff's license
18 available for distribution and reproduction via the BitTorrent protocol, I downloaded and retained
19 both the torrent files and the actual digital reproductions being offered for distribution to verify that
20 the digital copies being distributed in the swarm were in fact copies of the copyrighted creative
21 works subject to Plaintiff's license. Because a file could be mislabeled, corrupt or otherwise not an
22 actual copy of Plaintiff's files, I physically downloaded the file and compared it to an actual copy of
23 the copyrighted creative works to confirm that the file was a substantially-similar reproduction of the
24 copyrighted creative work.

1 20. Finally, I stored all of the data we collected in a central database for later use,
2 examination and audit.

3 **The Critical Importance of Expedited Discovery**

4 21. Defendants are known to Plaintiff only by the IP number they were assigned by their
5 Internet service provider on the date and time we observed each Defendant engaging in infringing
6 conduct. The only party from whom Plaintiff can discover Defendant’s actual names and addresses
7 is Defendant’s Internet service provider. Without expedited discovery in this case against
8 Defendant’s Internet service provider, Plaintiff will have no means of serving Defendants with the
9 complaint and summons in this case and no means to protect its creative works from ongoing
10 infringement.

11 22. Internet services providers have different policies regarding the length of time they
12 preserve information about what IP address was associated with a given subscriber at a given date
13 and time. Some Internet service providers store this information for as little as weeks or even days
14 before potentially permanently erasing the data they contain. Informal requests for data preservation
15 to Internet service providers can meet with varying degrees of success and are no substitute for
16 formal discovery. If an Internet service provider does not have to respond efficiently to a discovery
17 request, the information in that ISP’s database may be erased forever.

18 23. Certain ISPs own excess IP addresses that they lease or otherwise allocate to third
19 party “intermediary ISPs.” Because the lessor ISP has no contractual relationship with the
20 intermediary ISP’s customers, the leasing ISP would be unable to identify the Doe Defendants
21 through reference to their user logs. In contrast, the intermediary ISP should be able to so identify.

22 **Continued Monitoring**

23 24. The copyrighted creative works at the heart of this action continue to be made
24 available for unlawful duplication and distribution via the BitTorrent protocol, in violation of
25

1 Plaintiff's exclusive license to reproduce and distribute the copyrighted works via the BitTorrent
2 protocol. MCG continues to monitor on a real time basis the unlawful duplication and distribution
3 and to identify content pirate by the unique IP address assigned to them by their respective Internet
4 Service Providers on the date and at the time of the infringing activity.
5

6
7 Executed on April 1, 2011, in Minneapolis, MN.

8
9 

10
11 _____
12 Peter Hansmeier
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28