

1 D. Gill Sperlein (SBN 172887)
2 THE LAW OFFICE OF D. GILL SPERLEIN
3 345 Grove Street
4 San Francisco, California 94102
5 Telephone: (415) 404-6615
6 Facsimile: (415) 404-6616
7 gill@sperleinlaw.com

8 Attorney for Plaintiff Celestial, Inc.

9 UNITED STATES DISTRICT COURT
10 CENTRAL DISTRICT OF CALIFORNIA

11 CELESTIAL, INC,

12 Plaintiff,

13 vs.

14 SWARM SHARING HASH
15 8AB508AB0F9EF8B4CDB14C624
16 8F3C96C65BEB882 ON
17 OCTOBER 27, 2011 and DOES 1
18 and 2,

19 Defendants.

) CASE NO.: 12-CV-00128 DDP (SSx)

)
)
) DECLARATION OF TOBIAS FIESER
) IN SUPPORT OF PLAINTIFF'S
) MOTION FOR LEAVE TO TAKE
) DISCOVERY PRIOR TO RULE 26
) CONFERENCE

) DISCOVERY MATTER

) Date: March 5, 2012

) Time: 10:00 a.m.

) Judicial Officer: Hon. Dean Pregerson

) (But submitted on record)

21
22
23 I, Tobias Fieser, declare:

24 1. The facts that I state herein are within my personal knowledge, I know
25 the same to be true, and if called upon to testify I could and would.
26
27
28

1 2. I am the Director of Data Services for IPP International UG (IPP), a
2
3 company incorporated in Germany under company number 115546. IPP is a
4 provider of online anti-piracy services for the motion picture industry. IPP is the
5 leading provider of online anti-piracy services for the motion picture industry.
6

7 3. I have been employed with IPP since 2010. Before employment with
8 IPP, I held various software developer and consultant positions at companies where
9 I specialized in filesharing technologies. I have nearly seven years experience
10 related to protocols, technical architecture, and operation of the Internet and
11 filesharing technologies.
12

13
14 4. At IPP, I am the head of the department that carries out evidence
15 collection and provides litigation support services. I work closely with our research
16 team to create credible and reliable processes to scan for, detect, and download
17 copies of infringed material on multiple network protocols for use by copyright
18 owners. I have a strong understanding of P2P technology, a method by which users
19 (peers) may download to their computers software that allows them to locate and
20 transfer files to and from other users/peers. In order to use the software to locate
21 and exchange files, a user/peer must first connect to the Internet.
22
23

24
25 **The Nature of Bit Torrent Technology**
26

27 5. While the Internet affords the unparalleled opportunity to exchange
28 vast amounts of important information, it also affords opportunities for the wide-

1 scale infringement of copyrighted motion pictures. Once transformed into an
2 unsecured digital format, infringers can further reproduce and distribute a movie
3 over the Internet an unlimited number of times without significant degradation in
4 picture or sound quality.
5

6
7 6. To reproduce and distribute motion pictures over the Internet, many
8 individuals use online media distribution systems commonly referred to as “peer-to-
9 peer” (P2P) networks. P2P networks are computer systems that enable Internet
10 users to make files on their computers available to others, search for files stored on
11 other users’ computers, and transfer exact copies of files from one computer to
12 another via the Internet. “BitTorrent” protocol or “torrent” is different from the
13 standard P2P protocol used for such networks as KaZaa and Limewire. BitTorrent
14 protocol makes even small computers with low bandwidth capable of participating
15 in large data transfers across a P2P network.
16
17

18
19 7. First, in a process called “seeding”, an initial file-provider shares a file
20 with P2P networks. Other users (“peers”) on the network connect to the seed file to
21 download. However, unlike a traditional P2P network, each new file downloader
22 receives a different piece of data from each user who has already downloaded the
23 file that together comprises the whole. This piecemeal system with multiple pieces
24 of data coming from different peer members is called a “swarm”. As new peers
25 request the same file, each new peer becomes a part of the network and the peers
26
27
28

1 offer parts of the file stored on his computer to other peers. This means that every
2 “node” or peer who has a copy of the infringing copyrighted material also becomes
3 a source of download for that infringing file.
4

5 8. Once connected, the program begins coordinating the copying of a file
6 among participating computers. As the system copies pieces of a file to a peer’s
7 computer, the system immediately makes those pieces available to other connected
8 peers seeking to obtain the file. The distributed nature of BitTorrent leads to a rapid
9 viral spreading of a file throughout peer users. As more peers join the swarm, the
10 efficiency, speed, and likelihood of a successful download increases.
11
12

13 9. In order to engage in the reproduction and distribution of a file such as
14 a movie, each participating peer obtains a reference file from the video index of a
15 BitTorrent website and loads that reference file into a computer program designed to
16 read such files. With a reference file loaded, the BitTorrent program employs the
17 BitTorrent protocol to initiate simultaneous connections to hundreds of other peers
18 possessing and sharing pieces of the movie described in the reference file. The
19 system tracks each file exchanged in this manner by creating a unique HASH ID.
20
21

22 10. Because of the nature of a P2P network, any peer who has downloaded
23 a part of the file prior to the time a subsequent peer downloads the same file is a
24 possible source for the subsequent peer as long as that first peer is online at the time
25 the subsequent peer begins to download the file.
26
27
28

1 11. IPP has licensed a proprietary technology that enables it to detect and
2 monitor the unauthorized transfer and distribution of files among P2P networks by
3 different protocols. Celestial, Inc. engaged IPP to detect and record the IP addresses
4 of individuals who, without authorization, reproduced and distributed its movies
5 using P2P technologies. IPP employed specially designed software technology to
6 identify direct infringers of Celestial's works. IPP documented evidence of
7 unauthorized reproduction and distribution of Celestial's works within the United
8 States, including California.
9
10

11
12 12. The claims identified in the Complaint involve peers who shared the
13 same unique HASH ID on the same day.
14

15 13. IPP used the search function of the P2P network to look for peers who
16 offered for distribution audiovisual files labeled with the name of Plaintiff's
17 copyrighted motion picture. IPP downloaded and carefully reviewed the file and
18 recorded the algorithmically created unique hash ID the system assigned the file.
19 Having confirmed that the hash ID identified Plaintiff's motion picture, IPP
20 commenced searching for peers making the content available for distribution. IPP
21 downloaded a part of the file and recorded the Internet Protocol (IP) address the peer
22 used to access the Internet and other specific information in order to confirm the
23 peer was distributing Plaintiff's movie.
24
25
26
27
28

1 14. Once IPP's searching software program identified a peer distributing
2
3 Plaintiff's work as described herein, IPP obtained and recorded publically available
4 information about the peer that is designed to help Plaintiff identify the infringer.
5 Among other things, IPP downloads or records for each file downloaded: a) the time
6 and date at which the peer distributed the file or a part of the file; b) the IP address
7 the peer used to access the Internet at the time of distribution; and in some cases c)
8 the video file's metadata (digital data about the file), such as title and file size, that
9 is not part of the actual video content, but that is attached to the digital file and help
10 identify the content of the file. IPP then creates evidence logs for each user and
11 store all this information in a database.
12
13
14

15 The Need for Expedited Discovery

16
17 15. Obtaining the identity of the subscribers assigned the IP addresses the
18 peers used to access the Internet and distribute Plaintiff's movie is critical to the
19 prosecution of this action. Without such discovery, Plaintiff has no way of
20 identifying and serving Defendants with the Complaint and Summons. Plaintiff
21 does not have Defendants' names, addresses, e-mail addresses, or any other way to
22 identify or locate Defendants, other than the unique IP address the peer used to
23 access the Internet and engage in the infringing conduct.
24
25
26

27 16. Individuals gain access to the Internet through an Internet service
28 provider (ISP). When an ISP provides Internet access to a subscriber, it does so

1 through a modem at the location the subscriber uses to access the Internet, usually
2 the home or office. An ISP can be a telecommunications service provider such as
3 Verizon, an Internet service provider such as America Online, a cable Internet
4 service provider such as Comcast, or even an entity such as a university that is large
5 enough to establish its own network and link directly to the Internet.
6
7

8 17. Each time the subscriber accesses the Internet, the ISP provides a
9 unique number to the subscriber called an Internet Protocol (IP) address. This is
10 somewhat akin to a telephone number. The IP address for a subscriber may stay the
11 same over time (a static IP address) or it may change from time to time (a dynamic
12 IP address). Most ISPs record in user logs the times and dates it assigns each IP
13 address to a subscriber.
14
15

16 18. P2P technologies, including the BitTorrent protocol, rely on the ability
17 to identify the computers to and from which peers search and exchange files. The
18 software used by peers identifies the computers of other peers via the IP address
19 through which the peer connected to the Internet. IPP identified the IP addresses of
20 individuals who connected to the Internet to distribute the file or pieces of the file
21 containing Plaintiff's copyrighted movie.
22
23

24 19. The IP addresses IPP identified for Plaintiff enable us to determine
25 which ISP each peer used to gain access to the Internet. Anyone can perform a
26 simple search on public databases to determine which Internet access provider
27
28

1 controls a specific IP address. However, some ISPs lease or otherwise allocate
2 certain of the IP addresses to other unrelated, intermediary ISPs. Since these ISPs
3 consequently have no direct relationship with the subscriber, they are unable to
4 identify user information. The intermediary ISPs' own user logs, however, should
5 permit identification of the subscribers. For this reason, Plaintiff may be required to
6 serve a second subpoena on an intermediary ISP. We determined that the potential
7 defendants here were using those ISPs listed in Exhibit A, attached hereto together
8 with other ISPs operating both within and outside California, to gain access to the
9 Internet to reproduce and distribute Plaintiff's copyrighted motion picture.
10
11
12
13

14 20. In my experience, Internet service providers maintain subscriber
15 activity logs indicating which of its subscribers were assigned an IP address at any
16 given date and time, but only maintain subscriber activity logs for a short period of
17 time before destroying the information contained in the logs. If an ISP does not
18 have to respond expeditiously to a discovery request, the ISP may destroy the
19 identification information stored in the ISP's logs.
20
21

22 21. I am aware of no reliable means for identifying the DOE Defendants in
23 this matter other than obtaining subscriber information for IP addresses associated
24 with the infringing activity from Internet service providers.
25
26
27
28

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

Conformation of Downloaded Material

22. My responsibilities at IPP include confirming that the digital audiovisual files downloaded by IPP are actual copies of Plaintiff's motion picture. It is possible for peers to mislabel digital files either accidentally or on purpose, and sometimes, digital files are corrupted. Therefore, IPP (and accordingly Plaintiff) does not rely solely on the labels and metadata attached to the files to determine which motion picture the downloaded file contains, but also confirms the content through a visual comparison between the downloaded file and a legitimate copy of the motion picture.

23. As to Plaintiff's copyrighted motion picture identified in the Complaint, I or one of my assistants have watched a DVD copy of the motion picture provided by Plaintiff. After IPP identified the peers and downloaded the motion picture they distributed, we opened the downloaded files, watched them, and confirmed that they contain a substantial portion of the motion picture identified in the Complaint.

Pursuant to the laws of the United States, I declare under penalty of perjury the foregoing is true and correct.

Dated: 31st January 2012

Tobias Fieser
TOBIAS FIESER
IPP International UG