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

Attorney for Petitioner

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF CALIFORNIA

In the Matter Of a Petition By INGENUITY13 LLC,	**No.** Judge: **VERIFIED PETITION TO PERPETUATE TESTIMONY**

1. Petitioner Ingenuity13 LLC by and through its undersigned attorney, hereby petitions this Court for an order pursuant to Federal Rule of Civil Procedure 27 authorizing the issuance of subpoenas *duces tecum* to the Internet Service Providers ("ISPs") listed on Exhibit A to this petition.

2. Petitioner is limited liability company organized and existing under the laws of the Federation of Saint Kitts and Nevis. Petitioner produces adult entertainment content and this content is being unlawfully reproduced and distributed over the Internet via the BitTorrent file transfer protocol. An individual or individuals wrongfully reproduced and distributed Petitioner's copyrighted works via the BitTorrent protocol in violation of Petitioner's exclusive rights under United States Copyright Act, 17 U.S.C. §§ 101, *et seq*. Petitioner anticipates bringing a civil action against the person or persons engaging in such unlawful activity. This action would be cognizable in a United States court as United States courts have exclusive jurisdiction over copyright actions. Without knowing the identity or identities of the anonymous infringers, Petitioner has no means to

name and serve the individual or individuals in an action with summons and complaint. The purpose of this petition is to ascertain these identity or identities.

3. Petitioner seeks the name, address, telephone number, e-mail address and Media Control Access number of each account holder associated with the Internet Protocol ("IP") addresses listed on Exhibit B to this petition. Each of the IP addresses was identified by Petitioner's agents as being associated with infringing activity on the corresponding dates and times listed on Exhibit B. The reasons to perpetuate the testimony are multiple. First, without this information Petitioner has no means to name and serve a complaint on the infringing parties. Second, on information and belief, this information is destroyed in the regular course of business and will be unavailable to Petitioner after it is destroyed. An example of an ISP's data retention policy is shown as Exhibit C. Finally, under the Cable Communications Policy Act, 47 U.S.C. § 551(c)(2)(B), a court order is necessary to discover an account holder's identity.

4. The names and addresses of the person or persons whom Petitioner expects to be adverse parties are unknown to Petitioner. The individual or individuals responsible for infringing Petitioner's works are known to Petitioner only by an IP address—a number that is assigned to devices, such as computers, that are connected to the Internet. Petitioner used geolocation to trace the IP addresses of the expected adverse party or parties to a point of origin within the State of California.

5. The name and address of each responding party is set forth on Exhibit A to this petition. Petitioner is seeking the name, address, telephone number, e-mail address and Media Control Access number of each account holder associated with the Internet Protocol ("IP") addresses listed on Exhibit B to this petition.

FACTUAL ALLEGATIONS

6. Petitioner is the owner of the copyright for the motion picture set forth in Exhibit D to this petition.

7. As set forth below, Petitioner has actionable claims for direct and contributory copyright infringement and a claim for civil conspiracy against the individual or individuals who

engaged in infringing activities via the IP addresses set forth on Exhibit B hereto based on the parties' use of the BitTorrent protocol to illegally reproduce and distribute Petitioner's work(s).

A. The Unknown Infringers used BitTorrent to Infringe Petitioner's Copyrights

8. BitTorrent is a modern file sharing method ("protocol") used for distributing data via the Internet. BitTorrent protocol is a decentralized method of distributing data. Instead of relying on a central server to distribute data directly to individual users, the BitTorrent protocol allows individual users to distribute data among themselves by exchanging pieces of the file with each other to eventually obtain a whole copy of the file. When using the BitTorrent protocol, every user simultaneously receives information from and transfers information to one another.

9. The BitTorrent protocol is an extremely popular method for transferring data. A group of individuals transferring data among one another (the "swarm") will commonly include peers from many, if not every, state in the United States and several countries around the world. And every peer in the swarm participates in distributing the file to dozens, hundreds, or even thousands of other peers.

10. The BitTorrent protocol is also an extremely popular method for unlawfully copying, reproducing, and distributing files in violation of the copyright laws of the United States. A broad range of copyrighted albums, audiovisual files, photographs, software, and other forms of media are available for illegal reproduction and distribution via the BitTorrent protocol.

11. Efforts at combating BitTorrent-based copyright infringement have been stymied by BitTorrent's decentralized nature. Because there are no central servers to enjoin from unlawfully distributing copyrighted content, there is no primary target on which to focus anti-piracy efforts. Indeed, the same decentralization that makes the BitTorrent protocol an extremely robust and efficient means of transferring enormous quantities of data also acts to insulate it from anti-piracy measures.

12. The infringing parties in this action were all observed using the BitTorrent protocol to unlawfully reproduce and distribute Plaintiff's copyrighted work by exchanging pieces with one another either directly or via a chain of data distribution.

B. Each infringer installed a BitTorrent Client on his or her computer

13. The individual or individuals associated with the infringing activity installed a BitTorrent Client onto his or her computer(s). Normal commercial computers do not come pre-loaded with BitTorrent software. Each infringer must have separately installed on their respective computers special software that allows peer-to-peer sharing of files by way of the Internet. The infringers use software known as BitTorrent clients. Among the most popular BitTorrent clients are Vuze (formerly Azureus), µTorrent, Transmission and BitTorrent 7, although many others are used as well.

14. Once installed on a computer, the BitTorrent "Client" serves as the user's interface during the process of uploading and downloading data using the BitTorrent protocol.

C. The Initial Seed, Torrent and Tracker

15. A BitTorrent user who wants to upload a new file, known as an "Initial Seeder," starts by creating a "torrent" descriptor file using the client he or she installed onto his or her computer. The Client takes the target computer file, the "initial seed," in this case, one of the copyrighted Works, and divides it into identically sized groups of bits known as "pieces." The Client then gives each one of the computer file's pieces, in this case, pieces of one of the copyrighted works, a random and unique alphanumeric identifier known as a "hash" and records these hash identifiers in the torrent file.

16. When another peer later receives a particular piece, the hash identifier for that piece is compared to the hash identifier recorded in the torrent file for that piece to test whether the piece is free of errors. In this way, the hash identifier works like an electronic fingerprint to identify the source and origin of the piece and ensure that the piece is authentic and uncorrupted.

17. Torrents files also have an "announce" section, which specifies the Uniform Resource Locator ("URL") of a "tracker" and an "info" section, containing (suggested) names for the files, their lengths, the piece length used, and the hash identifier for each piece, all of which are used by the Client on peer computers to verify the integrity of the data they receive. The "tracker" is a computer or set of computers that a torrent file specifies and to which the torrent file provides

peers with the URL address(es). The tracker computer or computers direct a peer user's computer to another peer user's computer that have particular pieces of the file, in this case, one of the copyright Works on them, and facilitates the exchange of data among the computers. Depending on the BitTorrent Client, a tracker can either be a dedicated computer (centralized tracking) or each peer can act as a tracker (decentralized tracking).

D. Torrent Sites

18. "Torrent Sites" are websites that index torrent files that are currently being made available for copying and distribution by the people using the BitTorrent protocol. There are numerous torrent websites, such as www.torrentz.eu or thepiratebay.org.

19. Upon information and belief, each infringer went to a torrent site to upload and download one of the Petitioner's copyrighted Works.

E. Uploading and Downloading a Work Through a BitTorrent Swarm

20. Once the initial seeder has created a torrent and uploaded it onto one or more torrent sites, then other peers begin to download and upload the computer file to which the torrent is linked (here, one of the copyright Works) using the BitTorrent Client that the peers installed on their computers.

21. The BitTorrent protocol causes the initial seed's computer to send different pieces of the computer file, here, one of the copyrighted Works, to the peers who are seeking to download the computer file. Once a peer receives a piece of the computer file, it starts transmitting that piece to other peers. In this way, all of the peers and seeders are working together in what is called a "swarm."

22. Here, each infringing peer member participated in a swarm through digital handshakes, the passing along of computer instructions, uploading and downloading, and by other types of transmissions.

23. In this way, and by way of example only, one initial seeder can create a torrent that breaks a movie up into hundreds of piece saved in the form of a computer file, like the Works here, upload the torrent file onto a torrent site, and deliver a different piece of the computer

file to each of the peers. The receiving peers then automatically begin delivering the piece they just received to the other peers in the same swarm.

24. Once a peer, here an infringer, has downloaded the full file, the BitTorrent Client reassembles the piece and the peer is able to view the video. Also, once a peer has downloaded a full file, that peer becomes known as "an additional seed" because it continues to distribute the torrent file which, in this case, was one of the copyrighted Works.

F. Petitioner's Computer Investigators Identified Each Infringer's IP Address as an Infringer of Petitioner's Copyright Works

25. Petitioner retained 6881 Forensics, LLC ("6881") to identify the IP addresses used by the individual or individuals that were misusing the BitTorrent protocol to unlawfully distribute Petitioner's copyrighted Work.

26. 6881 used forensic software, "BitTorrent Auditor" to audit a swarm for the presence of infringing transactions.

27. 6881 extracted the resulting data gathered from the investigation, reviewed the evidence logs, and isolated the transactions and the IP addresses associated with the copyrighted work listed on Exhibit D hereto.

28. The IP addresses and hit dates contained on Exhibits B accurately reflects what is contained in the evidence logs and show that:

(A) Each infringer copied a piece of one of Petitioners copyrighted work; and

(B) Each infringer was part of a BitTorrent swarm.

29. 6881's technician analyzed each BitTorrent "piece" distributed by the IP addresses listed on Exhibit B and verified that each piece consisted of part of the copyrighted work.

30. In order for petitioner to be able to take appropriate action to protect its copyrighted work under 17 U.S.C. §§ 101, *et seq*, petitioner must be authorized issuance of subpoenas *duces tecum* to the ISPs listed on Exhibit A to this petition.

31. No prior application has been made for the relief sought herein.

WHEREFORE, petitioner requests that an order be made and entered directing that petitioner may compel the production of documents to the extent of determining the name, current (and permanent) addresses, telephone numbers, e-mail addresses and Media Access Control addresses of the person or persons whose IP addresses are listed in Exhibit B from the ISPs listed on Exhibit A for the purposes of determining the true identity of unknown infringers. To further support its Petition, Petitioner attaches as Exhibit F its Memorandum of Law in Support of Petitioner's Verified Petition to Perpetuate Testimony.

Respectfully Submitted,

Ingenuity13 LLC,

DATED: October 28, 2011

By: /s/ Brett L. Gibbs, Esq.

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

NOTARIZED VERIFICATION

I declare under penalty of perjury under the laws of the United States of America that the foregoing information contained in this Verified Petition is, to the best of my knowledge, true and correct.

DATED: October 28, 2011

_____/S/_ Alan Cooper_____
Alan Cooper, Manager of Ingenuity 13 LLC

I, Brett L. Gibbs, Esq., hereby confirm per Eastern District of California Local Rule 131(f) that counsel for Plaintiff has a signed original notarized version of the above Verified Petition.

DATED: October 28, 2011

By: _____/s/ Brett L. Gibbs, Esq._____

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