EXHIBIT A

1 2 3 4 5 6 7 8	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 IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA SAN FRANCISCO DIVISION
10 11 12 13 14 15	AF HOLDINGS LLC, Plaintiff, v. DOES 1-96, Defendant. SUPPLEMENTAL DECLARATION OF PETER HANSMEIER ADDRESSING FOR FURTHER DECLARATION SUPPLEMENTAL DECLARATION OF PETER HANSMEIER ADDRESSING THE
17 18 19 20 21 22 23 24 25 26 27 28	I, Peter Hansmeier, declare under penalty of perjury as true and correct that: 1. I am a technician at Media Copyright Group, LLC ("MCG"). On behalf of its clients, MCG monitors and documents Internet-based piracy of our clients' copyrighted creative works. I submit this supplemental declaration in response to the Court's July 27, 2011 Order Requesting Further Declaration from Plaintiff relating to its <i>Ex Parte</i> Application for Leave to Take Expedited Discovery, and, specifically, on three technical questions. 2. 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.
	SUPPLEMENTAL DECLARATION OF PETER HANSMEIER ADDRESSING THE COURT'S ORDER C-11-03335 JSC

QUESTION 1:

The Complaint states that "each defendant knew, should have known, or had some constructive knowledge that their acts constituted copyright infringement." (Dkt. No. 1 Pg. 7). What facts, specifically related to each Doe Defendant one through ninety-six, support this conclusory assertion? In particular, how might a Doe Defendant distinguish between the non-copyrighted work legitimately available through BitTorrent and Plaintiff's copyrighted work?

- 3. The Doe Defendants knew or should have known that Plaintiff's work was not legally redistributable for multiple independently sufficient reasons. First, the torrent files that the Doe Defendants downloaded to access Plaintiff's work contained the name of Plaintiff's work, "Sexual Obsession." A simple Google search for "Sexual Obsession DVD" reveals that Sexual Obsession is a copyrighted DVD retailing for approximately \$24.99.
- 4. Second, the torrent sites that the Doe Defendants downloaded the torrent files from are notorious digital piracy sites. For example, one of the sites used by the Doe Defendants to enter the swarm related to this suit was the aptly-named, "Pirate Bay" (pirate, of course, is an Internet colloquialism for someone who uses the Internet to unlawfully access files). An individual would have to be thoughtful in order to *avoid* downloading a copyrighted work via one of these sites. In contrast to torrent sites notorious for this nefarious behavior, there are other legitimate websites, such as Mininova.org, that aim to only allow legally redistributable media. Individuals downloading Plaintiff's video on "Pirate Bay," understand the connotations of their actions.
- 5. Third, the torrent file download page, which would have been viewed by the individuals who opted to download this particular file, contained a description of the work for download. It read, in part¹, "Sexual Obsession Heartbreaker Films. Featuring Sophia Santi in her first XXX boy girl DVD!..." The description also contained the names of all of the actors and actresses in the video. Among the listed names were Sophia Santi and Nina Mercedez—adult

¹ Out of respect for the decorum of this Court, I refrain from repeating the description in its entirety as certain parts of the description are quite explicit in nature and not relevant to whether the work would have been perceived as copyrighted. Needless to say, it was a full description of the exact video the individual intended to download.

industry stars who make their living by appearing in copyrighted works. Further, the description contained website links to box cover art (which clearly denoted a copyrighted work) as well as screen captures from the video.

6. If an individual was genuinely interested in distinguishing a copyrighted work that was legally distributable from a copyrighted work that was not legally distributable then the individual would first avoid sites that were notorious for copyright infringement, double check the torrent file name to confirm that the work is not associated with a commercial copyrighted work and then review the description on the torrent file download page to confirm the same. These small tasks would be very simple for anyone with an Internet-ready computer (i.e. anyone who could download the video via BitTorrent in the first place) to complete in order to protect themselves from being involved in infringing conduct.

QUESTION 2:

Plaintiff's Complaint further alleges that "Doe Defendants' conduct was willful with the meaning of the copyright Act... Doe Defendants' active participation on BitTorrent swarms relating to Plaintiff's Work make this fact abundantly clear." (Dkt. No. 1, Pg. 8). Can Plaintiff articulate facts about the different activity levels of each Doe Defendant? For example, is it possible to differentiate between Doe Defendants who joined the swarm from the chat rooms and downloaded the entire file in question versus those who might have stumbled on the file in question, joinded the "swarm" only momentarily, and not completed the download of the entire file?

7. This question appears to imply that BitTorrent users might be able to simply stumble across a BitTorrent file, much as one might stumble across a YouTube video linked to from a forum. For the sake of clarity, however, it would be rather unusual to inadvertently download a file on BitTorrent (so long as the file was not misleadingly named). In other terms, while viewing a YouTube video could be characterized as an inadvertent action under certain circumstances, downloading a file on BitTorrent can only be characterized as a calculated action in light of the preceding stages undertaken prior to downloading the video.

- 8. Using BitTorrent is quite plainly a deliberate action. First, the individual must download BitTorrent, and install the protocol to its computer. Second, in order to download a video via BitTorrent, one must first visit a torrent indexing site to locate a torrent file. These torrent indexing sites have a variety of copyrighted videos for infringing like going to a black-market video store, and selecting a video off of a list of those available, except here there is obviously no payment involved. A torrent file is a small (~40kb) file that contains directions to the swarm and a fingerprint of the underlying video to be downloaded. Then the user must load the torrent file into (previously downloaded) BitTorrent software. In other words, the process of obtaining a file via BitTorrent is far more complex than merely streaming a video via YouTube.
- 9. To the Court's question, I believe that our software allows us to distinguish between the hypothetical peer that "momentarily" joined the swarm and a genuine participant in the swarm. Specifically, I believe that our software allows us to identify genuine participants in the swarm by virtue of not only recording the IP addresses of the swarm participants, but also recording their activity in the swarm.

QUESTION 3:

Plaintiff alleges that "Doe Defendants, without authorization, used an online P2P media distribution system to download Plaintiff's copyrighted works and distribute Plaintiff's copyrighted works to the public, including making Plaintiff's copyrighted works available for distribution to others." (Dkt. No. 6, Pg. 3). Does Plaintiff have information, based on the amount of time certain ISP [sic] addresses were part of the "swarm" or other indicia, on conduct particular to each Doe Defendant in regard to whether each downloaded the entire file and whether each participated in distributing this work to others in the swarm? In other words, can Plaintiff's software capture any information other than the mere presence of an ISP [sic] address within a swarm?

10. As described above, Plaintiff's software captures more information than merely the IP addresses of swarm participants. In particular, the software captures a list of peers in the swarm (by IP address), logs the <u>BitTorrent-protocol messages</u> broadcast by the peers and receives a piece of the file from the peers. To be clear, in this case we identified more potential peers (by IP address) than

Plaintiff ultimately named in its complaint.² The reason for this is that capturing the BitTorrent-protocol messages allows us to validate that the IP addresses we log in the swarm are actual peers in the same, single swarm, uploading/downloading the same exact file amongst themselves, and allows us to understand what type of activity each peer was engaged in.

11. By way of background, BitTorrent-protocol messages are messages that BitTorrent software communicates to other peers in a swarm. By analyzing the BitTorrent protocol messages broadcast by a given peer, we can discern some or all of the following (depending on the type of messages received): 1) what pieces of the file the peer had downloaded; 2) how much of the file the peer had downloaded; 3) what pieces the peer was offering to share; and 4) what pieces the peer was requesting from our software. We can discern other information as well, but the foregoing categories of information go most directly to the Court's area of interest.

Executed on August 12, 2011, in Minneapolis, MN.

Peter Hansmeier

² In this manner I believe that our software *may* differ from the software used by other piracy-monitoring organizations. Although I do not have personal knowledge of the mechanics of the software used by other monitoring organizations, media reports have suggested that the software used by other organizations captures only lists of IP addresses. Although merely capturing IP addresses may allow a Plaintiff to name more defendants in a given suit, it also introduces the risk of false positives. For a variety of technical reasons, capturing BitTorrent-protocol messages from peers provides a high degree of validation of presence in the swarm. While relying on high levels of validation may not allow Plaintiff to name thousands of peers in a single suit, such validation does give Plaintiff a high degree of confidence that an IP address identified as participating in the swarm was indeed engaged in infringing activity.