

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF TEXAS  
DALLAS DIVISION**

MICK HAIG PRODUCTIONS, E.K.,	§	
HATTINGER STR. 88	§	
D-44789 BOCHUM, GERMANY,	§	
	§	
PLAINTIFF,	§	
	§	
VS.	§	
	§	
DOES 1-670	§	C.A. NO.: 3:10-cv-01900-N
	§	
DEFENDANTS.	§	

**DECLARATION OF MATTHIAS SCHRÖDER-PADEWET IN SUPPORT OF  
PLAINTIFF’S MOTION FOR LEAVE TO TAKE DISCOVERY  
PRIOR TO RULE 26(f) CONFERENCE**

I, Matthias Schröder-Padewet, declare:

1. I am the President of Excubitor USA, Inc. (“Excubitor”), a company registered in the United States. I have over 10 years of experience in the area of digital media and computer technology.
2. I submit this declaration in support of Plaintiff’s Motion for Leave to Take Discovery Prior to Rule 26(f) Conference. 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 head a team that is responsible for researching and developing systems for validation and recording of copyright infringement occurring publicly via the internet. My team and I also provide technical litigation support.
4. Excubitor, uses a licensed, proprietary technology to track unauthorized reproduction and distribution of copyrighted works over the internet—specifically, that which is carried out using

the BitTorrent protocol. The process of distributing a particular work with this protocol commences with one user intentionally making a digital embodiment of the work available to the public. This first file is known as a “seed.” Persons seeking to unlawfully download such media seek it out via a reference file called a “torrent” file, which describes the media and the path by which it can be obtained. With the availability of the seed, other users (“peers”) requesting the same file engage the seed and engage each other in a group known as a “swarm,” and begin downloading some portion of the seed. In turn, as each peer receives portions of the seed, they make those pieces available to other peers in the swarm. Therefore, each peer in the swarm is both copying and distributing copyrighted material at the same time. As new peers join the swarm, they obtain the content at even greater speeds because of the increasing number of peers simultaneously offering the content for unlawful distribution.

5. The Plaintiff in this action is Mick Haig Productions e.K. Plaintiff engaged Excubitor to document evidence of the unauthorized reproduction and distribution of the Plaintiff’s adult film, “Der Gute Onkel.” Excubitor thereafter collected and documented the evidence of infringement using the methods detailed below.

6. At regular intervals our licensed technology informs us about new torrent files offering the movie file, “Der Gute Onkel.” After notification, the torrent was opened and the offered data was downloaded. Subsequently we carefully reviewed the downloaded movie file and compared it to the original file provided by the Plaintiff. After a successful match of the both files we added the torrent to our monitoring software. Our licensed software started searching for individuals making the content available to the public. When an individual, a so-called “peer,” was located, a part of the file was downloaded and stored, as well as other specific protocol-related information in order to confirm and document the infringement. Each infringer is identified by the

unique Internet Protocol (“IP”) address, assigned to the infringer by his/her ISP on the date and time of the infringing activity.

7. IP addresses are numerical labels assigned to customers by an internet service provider such as Verizon, Time Warner Cable or Comcast and are often reassigned within short periods of time. The logs regarding such assignments, are likewise kept only for relatively short periods of time. The numeric encoding used in these labels provides for more than four billion possible IP addresses, which are allocated internationally by the Internet Assigned Numbers Authority. These addresses are allocated among countries and service providers and are publicly indexed in a way that correlates a certain range of numbers to a specific country and a certain sub-range of numbers to a specific internet service provider. After matching an IP address to the range belonging to a certain service provider, one can then inquire of the service provider which customer that specific IP address had been assigned to at a certain date and time in question. To determine which service providers were providing internet access to the people unlawfully distributing this film, we submitted the list of addresses we collected to a trusted, commercial IP lookup service. The service returned information pertaining to each address, including the service provider to which each particular address was allocated. This information along with all the other captured data was then archived on a secure server for safekeeping.

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

Executed on September 29, 2010 at my offices in Karlsruhe, Germany.



---

Matthias Schröder-Padewet