# EXHIBIT 3

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE SOUTHERN DISTRICT OF ILLINOIS**

| | | |
|---|---|---|
| OPENMIND SOLUTIONS, INC., | ) | |
| Plaintiff, | ) | |
| v. | ) | |
| DOES 1-2925 | ) | CA. 3:11-cv-00092-GPM-SCW |
| Defendants. | ) | |

## DECLARATION OF SETH SCHOEN

I, Seth Schoen, declare as follows:

1. I am a Senior Staff Technologist with the Electronic Frontier Foundation (EFF), and I make this declaration on my own personal knowledge. I have worked with computers and computer networks for over a decade, have testified about electronic communications systems in two courts and before the United States Sentencing Commission, and have submitted declarations similar to my present declaration to the Federal courts in at least seven other matters.

2. The purpose of this declaration is to set forth facts, which were readily available to Plaintiff from free, public Internet sources at and before the time it filed suit, that establish that many of the unnamed Defendants in the above-referenced case (hereinafter "Does" or "Doe Defendants") use Internet connections likely located physically outside of the State of Illinois.

3. By reviewing Exhibit A to the Complaint, I compiled a list of the Internet Protocol (IP) addresses that Plaintiff attributes to each of the Doe Defendants.

4. There are many tools freely available to the public that help reveal where a person using a particular IP address is likely to be physically located. This process is often referred to as "geolocation." This information is commonly used for many purposes, such as customizing the language or content of web sites based on inferences about where visitors are accessing the site

from. For example, Google, Inc., uses geolocation to choose to display its web site in German to people coming from Germany, in French to people coming from France, and so on. It also uses geolocation to display ads and results related to particular cities or regions to people accessing its site from those cities or regions.

5. One means of learning about where an IP address is physically located is known as "reverse domain name service lookup" or "reverse DNS." When an Internet service provider ("ISP") allocates or prepares to allocate IP addresses to customers, it typically creates and publishes database records assigning a human-readable "domain name" to each numerical IP address. The reverse lookup information can be obtained by anyone using a program such as "host," which is a standard program included with many computer operating systems, or with any of several web-based tools such as the DNS lookup service at <http://lookupserver.com/>.

6. One of the purposes of reverse DNS is to help interested parties learn more about what a computer is used for, what organization's network it is connected to, and, in many cases, where the computer is physically located. Typically, for home users of dial-up or broadband connections, such as DSL or cable-modem services, a domain name obtained from reverse DNS will identify which ISP assigned the IP address.

7. In addition, such a domain name will frequently incorporate an approximate physical location, such as the name of a municipal area, state, or region. For example, one of the Does being sued here – Doe Defendant #22, mentioned on page 1 of Exhibit A to the Complaint – is identified by the IP address 108.15.38.6 and described by Plaintiff as a subscriber of Verizon Online LLC. The reverse DNS database identifies this computer as pool-108-15-38-6.bltmmd.fios.verizon.net, confirming Plaintiff's suggestion that this Doe is a Verizon ("verizon.net") customer, likely using Verizon's FiOS fiber optic Internet service, but adding the additional detail that the likely physical location of the computer is in or near Baltimore, Maryland ("bltmmd"). This means that in all likelihood, the individual who used this IP address is located in the Baltimore area.

8. Although Internet service providers are not required to publish this information, and

although it is sometimes only given to state-level precision, it can, when available, be a useful source of data about where an individual Internet connection is most likely located.

9. I looked at 2925 IP addresses that were referenced in this suit. For each of the 2925 IP addresses alleged by Plaintiff to belong to a Doe defendant, I used the "host" program to perform a reverse lookup against the publicly-accessible reverse DNS service.

10. The results of this process generally confirmed Plaintiff's association of particular IP addresses with particular ISPs. Additionally, the results of this process generally strongly suggested a geographic location for most individual defendants. In other words, most of the Does listed in this lawsuit can be associated by the host reverse DNS look-up with both an Internet service provider and a geographic location.

11. Reverse DNS records indicate that Does in this lawsuit include customers with Internet connections located in virtually all areas of the United States, including some in or near Hawaii; Maine; Los Angeles, California; New York City; the Tampa Bay Area in Florida; Philadelphia, PA; Newark, NJ; Columbus and Cincinnati, OH; Washington, DC; and other states and regions throughout the United States.

12. In addition to reverse DNS information, another means of learning where an IP address is located is to use a public database operated by the American Registry for Internet Numbers ("ARIN database"). ARIN is the authority responsible for the initial allocation of IP addresses to ISPs located in the United States. ARIN maintains public records indicating to whom a given IP address has been allocated. Large ISPs may apply to ARIN multiple times to receive multiple "blocks" or ranges of IP addresses. Each such block may be dedicated to a particular purpose or geographic area.

13. The ARIN database can be searched using a public web site provided by ARIN at <https://www.arin.net/>, or by using a program called "whois," which is a standard part of some operating systems and performs the same database-searching function. There is no charge for searching the ARIN database.

14. For example, Doe Defendant #2688 is identified by the IP address 98.202.80.226. I

searched the ARIN whois database for this address and learned that this address is part of a network assigned to Comcast Cable Communications, Inc., and designated UTAH-19. This suggests that this network provides service to customers who are in the state of Utah. Both of these inferences are consistent with the reverse DNS record for this IP address, which is c-98-202-80-226.hsd1.ut.comcast.net.

15. In addition, several companies collect and continually update geographic information about IP address locations from a variety of data sources, and collect this information in databases called "geolocation databases." Geolocation databases are commonly used by web site operators who are interested in finding out the approximate physical location of their web visitors. Since web site operators are often very interested in such information, there is considerable demand for geolocation databases.

16. Geolocation databases may be sold or given away for free. One very popular geolocation database is the "GeoIP" database maintained by MaxMind, Inc., a Boston company that specializes in geolocation technology. In addition to other sources of information, MaxMind explains that it "employ[s] user-entered location data from sites that ask web visitors to provide their geographic location" in order to learn which IP address ranges correspond to which cities and states. MaxMind web site, <http://www.maxmind.com/app/ip-locate> (accessed January 12, 2011).

17. A version of the MaxMind GeoIP geolocation database is freely available for anyone to download from MaxMind. The company claims that this free version can determine the location of "79% [of U.S. IP addresses] within a 25 mile radius." MaxMind web site, <http://www.maxmind.com/app/geolitecity> (accessed March 11, 2011).

18. I downloaded this freely available database and looked up each Doe Defendant IP address in it, obtaining an estimated city and state location for each such address.

19. Because DSL and cable modem connections are provided from local hubs to users in a particular geographic region, there is good reason to believe that the geographic location data obtained by these methods actually reflects the physical location of the Internet connection, at

least in general terms. In other words, although geolocation data is not perfectly accurate, the geographic designations obtained by these methods likely indicate the approximate locations of the residences or other venues where the Does use their Internet-connected computers.

20. I have attached hereto as Exhibit A to this Declaration a list of the reverse DNS names of the Doe Defendants' IP addresses, as well as the estimated physical location of each such IP address according to the freely available version of the MaxMind GeoLite City database.

21. In my experience, computer professionals are generally aware of the existence and function of the reverse DNS and whois services, as well as geolocation databases such as the GeoIP database, and would use any or all of these sources of information when they needed to learn where a given IP address was physically located. These techniques are readily and easily available to Plaintiffs, their attorney, and to the computer professionals they have employed to perform the investigations leading to this lawsuit.

22. Though the MaxMind GeoLite City database and reverse DNS records are not perfectly accurate, I know of no reason to think that either source of information has a bias that makes it more or less likely that an individual IP address will appear to be located in Illinois.

23. From the information available from the MaxMind geolocation database, 111 (one hundred eleven) of the Doe Defendants appear to be located in the State of Illinois, 2772 outside of Illinois, and 42 are not assigned to any location by the database. This puts around 3.8% of the Doe Defendants in the State of Illinois, compared with the 4.1% of the population of the United States as a whole that resides in Illinois according to the 2010 Census.

24. Separately from the question of where Does reside, Plaintiffs did not submit all the details of the investigations that led them to accuse these Does of copyright infringement. These details could be important because simple methods of attempting to locate copyright infringers can easily go awry. For example, in 2008 researchers from the University of Washington found that, given then-prevalent methods for investigating BitTorrent transfers, it was straightforward to frame particular IP addresses for downloading files that they had not, in fact, ever attempted to download. The researchers experimentally framed their own laser printer and succeeded in

eliciting false allegations of copyright infringement against it. See Michael Piatek, Tadayoshi Kohno, and Arvind Krishnamurthy, "Challenges and Directions for Monitoring P2P File Sharing Networks, or, Why My Printer Received a DMCA Takedown Notice," in *Proceedings of the 3rd USENIX Workshop on Hot Topics in Security*, July 29, 2008, available at <http://www.usenix.org/event/hotsec08/tech/full_papers/piatek/piatek.pdf>.

25. Paragraphs 12-20 of the declaration submitted by Mr. Pfister in support of Plaintiff's motion for leave to take discovery describe a variety of data that Plaintiff's experts collected, using "proprietary" techniques. More detailed information about those techniques and copies of the data collected would be helpful to better understand the reliability of Plaintiff's expert's techniques and to explain why Plaintiffs believe that particular IP addresses are associated with infringing activities. To my knowledge, this information has not yet been submitted to this Court.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct and that this document was executed in San Francisco, California.

Dated: March 11, 2011 By: _____