IN THE UNITED STATES DISTRICT COURT FOR
THE WESTERN DISTRICT OF OKLAHOMA

Arista Records, LLC, et al., Plaintiffs,	§ § § §	
vs.	§	Case No. Civ-07-568-R
Does 1-11, Defendants.	§ § § §	

Declaration of Jayson E. Street
In Support of Defendants' Motion to Quash Subpoena

I, Jayson E. Street, under penalty of perjury, hereby declare and say that:

1) I am presently employed as Assistant Vice President of Information Security of MidFirst Bank in Oklahoma City, Oklahoma. My duties include but are not limited to the following:

   a) Network Security – Responsible for the installation, maintenance, backup/recovery, and monitoring of multiple Intrusion Detection Systems. Responsible for monitoring all company firewall systems. Provide security design and strategy input for network components and devices including Internet web servers, mail servers, routers, virtual private networks (VPN).

   b) Auditing, Policies and Procedures – Assist in developing new and maintaining existing policy and procedure documents.

Does Exhibit 3

c) Assist in development and implementation of internal Security Awareness activities. Work with external auditors to ensure the Bank is in compliance with regulations.

d) Investigations – Conduct computer forensic investigations as needed.

e) Projects have included, but are not limited to:

- Assisted in creating a segmented network infrastructure, using firewalls and Intrusion Prevention devices.
- Created and deployed a distributed wireless intrusion detection system to enforce a no WIFI policy.
- Created a process to deploy open source Network Intrusion Detection systems in a fast and efficient manner.
- Conducted several Pen Tests, in which the results have led to a more secured environment.
- Conducted several successful forensic investigations using EnCase and other tools.

2) I am also the Chief Information Security Officer of Stratagem 1 Solutions. Stratagem 1 Solutions is a business enterprise separate from MidFirst Bank.

a) As CISO for Stratagem 1 Solutions, I work with clients conducting penetration testing, consulting on the design of security systems and practices, and conducting research on emerging cyber threats.

b) I am well versed in the ten domains of Information Systems security defined by the International Information Systems Security Certification Consortium (ISC^2).

3) I specialize in intrusion detection response, penetration testing, and auditing.

4) I also have a working knowledge of the implementation and administration of major firewalls, vulnerability scanners, and intrusion detection systems.

5) In 2000, 2005, 2006 I consulted with the FBI and helped in the capture and successful prosecution of the criminals involved.

Does Exhibit 3

6) In 2001, COMPUBANK earned a 1 rating on a security audit by the OCC (Office of Comptroller of the Currency).

7) I have created and conducted security awareness training for COMPUBANK a major Internet bank in 2001 and have created security policies and procedures currently used by several companies such as El Paso Global Networks and MidFirst Bank.

8) At the request of the FBI, I was a guest speaker at the INFRAGARD 2004 wireless conference where I presented the current status of the hacking underground and issues concerning wireless security and some solutions to secure it.

9) In June of 2005, I spoke on the subject of the challenges of getting upper management to accept the information security process at the University of Advancing Technologies Tech Forum in Phoenix, Arizona.

10) In October of 2006, I was chosen as a key note speaker on the top five internet threats you don't hear enough about at the I.T. Summit in Tulsa, Oklahoma.

11) In January of 2007, I created and taught a three day training course on Intrusion Detection Systems for a government agency in Washington D.C.

12) In 2007, I consulted with the Secret Service on the WI-FI security posture at the White House.

13) My summary resume is submitted as ***Exhibit 4***.

14) I am a member of the board of directors of the Oklahoma INFRAGARD chapter (http://www.infragardok.org/), a member of the Open Source Vulnerability Data Base

Does Exhibit 3

("OSVDB")(http://www.osvdb.org.), and a member of the SNOSOFT Research Team (http://snosoft.com).

15) My main certifications are defined as follows:

a) **CISSP** (Certification for Information System Security Professional)
A certification reflecting the qualifications of information systems security practitioners. The CISSP examination consists of 250 multiple choice questions, covering topics such as Access Control Systems, Cryptography, and Security Management Practices, and is administered by the International Information Systems Security Certification Consortium or (ISC)2 (www.isc2.org). The (ISC)2 promotes the CISSP as an aid to evaluating personnel performing information security functions. From (https://www.isc2.org).

b) **GSEC** - GIAC Security Essentials Certification graduates have been taught the knowledge, skills and abilities required to incorporate good information security practice in any organization. The GSEC tests the essential knowledge and skills required of any individual with security responsibilities within an organization.

c) **GCIH** - GIAC Certified Incident Handlers (GCIHs) have the knowledge, skills, and abilities to manage incidents; to understand common attack techniques and tools; and to defend against and/or respond to such attacks when they occur.

d) **GCFA** - GIAC Certified Forensic Analysts (GCFAs) have the knowledge, skills, and abilities to handle advanced incident handling scenarios, conduct formal incident investigations, and carry out forensic investigation of networks and hosts. From SANS (www.giac.org).

Does Exhibit 3

e) **IEM** - NSA INFOSEC EVALUATION METHODOLOGY (IEM)

The IEM is the latest certification for FISMA. Two-day instructor-led, full participation course. The INFOSEC Evaluation Methodology (IEM) is a hands-on methodology for conducting evaluations of customer networks utilizing common technical evaluation tools. Students can expect to learn an easily repeatable methodology that provides each customer a roadmap for addressing their security concerns and increasing their security posture. This course is a follow on course to the popular National Security Agency's INFOSEC Assessment Methodology (IAM) and will result in an NSA certificate for those students meeting the appropriate qualifications.

f) **IAM** -NATIONAL SECURITY AGENCY-INFOSEC ASSESSMENT METHODOLOGY (IAM)

Specifically designed for FISMA compliance. This two-day instructor-led, full participation course is for experienced Information Systems Security analysts who conduct, or are interested in conducting INFOSEC assessments of information systems. The course teaches the NSA INFOSEC assessment process, a high-level, non-intrusive process for identifying and correcting security weaknesses in information systems and networks.

IAM was originally created by PDD-63 (now Homeland Security Presidental Directive-7) requirement for vulnerability assessments of automated information systems that support the U.S. Infrastructure. In addition to assisting the governmental and private sectors, an important result of supplying baseline standards for INFOSEC assessments is fostering a

Does Exhibit 3

commitment to improve an organizations security posture. The IAM is a prerequisite for the IEM Evaluation course. From (http://www.certtest.com).

g) **CCSE** - This certification is designed for network and security administrators who need to implement and maintain virtual private networks (VPN) with CheckPoint's FireWall-1. Intensive encryption, firewall and VPN skills are provided with this certification.

h) **CCSA** -This certification is designed for end-users and resellers who need a good technical understanding of VPN/FireWall-1 and need to install and set up simple configurations. From (http://certification.about.com).

i) **Security+**

The Security+ exam is designed for IT professionals who possess at least two years of experience working in a networked environment. It's also advisable to have some hands-on experience in the world of information security. A thorough working knowledge of TCP/IP networking is absolutely critical for success on the Security+ exam. Although it's not a formal prerequisite, CompTIA encourages Security+ candidates to complete the Network+ certification program prior to tackling the Security+exam. From (http://www.cramsession.com/articles/get-article.asp?aid=1071).

16) I have been asked by counsel for defendant(s) Doe(s) in the above-captioned law suit for my opinions on the accuracy of statements made by Carlos Linares, a representative of the Recording Industry Association of America, Inc. ("RIAA") and the Plaintiffs, filed on May 17,2007 as Document No. 7-2 in the case.

17) I have reviewed the following pleadings contained in the Court file in *Arista Records, LLC, et al. v. Does 1-11*, U.S. District Court for the Western District of Oklahoma, Case No. 07-568-R:

a) Plaintiffs' Complaint with Exhibit A, Document 1, filed May 17, 2007. Plaintiffs' Exhibit A is titled "Doe List," consists of pages 1- 12, and is marked Document 1-2.

b) Plaintiffs' declaration of Carlos Linares, the Vice President of the Recording Industry Association of America, Inc., document number 7-2, filed on May 17, 2007 in support of Plaintiffs' *Ex Parte* Application for Leave to Take Immediate Discovery.

18) I have also reviewed the Plaintiffs' Subpoena which bears a date of May 25, 2007 to Oklahoma State University with Attachment A (Doe 1-11 with IP addresses). I received Plaintiffs' Attachment A from Defendant(s) Doe(s) counsel. Plaintiffs' Attachment A was not filed by Plaintiffs in the Court's file.

19) The following publications support of my opinions:

a) ***Exhibit 5*** - Cisco Network Address Translation (NAT) Frequently Asked Questions Document ID 26704.

b) ***Exhibit 6*** – Sci-Tech November 23, 2003 article from CTA News Staff reporting a driver of a motor vehicle engaged in internet child pornography utilizing a laptop computer and Wi-Fi (wireless fidelity) card to crack into a computer in a nearby home.

c) ***Exhibit 7*** – Gartner 2006 Press Release Worldwide Antivirus Software Market Increased 13.6 Percent in 2005.

d) ***Exhibit 8*** – ARIN (American Registry for Internet Numbers) (IPv4 and IPv6) (1 page)

Does Exhibit 3

e) ***Exhibit 9*** - Packet Switching and the Internet (4 pages).

f) ***Exhibit 11*** – Press Release Strategy Analytics: Global Wireless Home Device Sales to Reach 314 Million Units by 2010, Boston, MA with graph of Wi-Fi and wireless productions.

20) I have reviewed the statements and opinions contained in the declaration of Carlos Linares filed by the Plaintiffs, document number 7-2, on May 17, 2007 in *Arista Records, LLC, et al. v. Does 1-11*, U.S. District Court for the Western District of Oklahoma. I disagree with representations and opinions offered by Plaintiffs' through their representatives the RIAA and Mr. Linares. I have addressed the most fundamental and the most problematic statements as they relate to identification of the Does.

21) Plaintiffs' witness Linares' declaration, at ¶ 12, states:

> "Users of P2P networks can be identified by their IP addresses because each computer or network device (such as a router) that connects to a P2P network must have a unique IP address within the Internet to deliver files from one computer or network device to another."

a). In my opinion, the above statement is factually erroneous.

b). The reasons for my opinion include but are not limited to:
An individual cannot be uniquely identified by an IP address. An IP address must be unique on a given network. However, networks of networks can have many duplicate addresses. A common technology called Network Address Translation (NAT) is used to present a single IP address from one network as the only address for all computers behind the control point (such as a router).[1]

[1]Cisco, Inc. Frequently Asked Questions submitted as ***Exhibit 5***, (http://www.cisco.com/en/US/tech/tk648/tk361/technologies_q_and_a_item09186a00800e523b.shtml#qa1): "Network Address Translation (NAT) is designed for IP address simplification and conservation. It enables

Any log capturing source IP addresses in a communication stream will only record the control point IP address. The actual IP address or any other device-specific identifiers are stripped away by the control point in the data stream and cannot be recorded by a mid-stream or end-point logging mechanism.

22) Plaintiffs' witness Linares' declaration, at ¶ 12, states:

"Two computers cannot effectively function if they are connected to the Internet with the same IP address at the same time."

a). In my opinion, the above statement is factually erroneous.

b). The reasons for my opinion include but are not limited to:
The Internet is a network of networks. Many computers can be connected to the Internet with identical IP addresses as long as they remain behind control points such as routers, fire walls, proxy servers, or similar technologies. NAT technology is required because the current IP addressing schema used on much of the Internet (IPv4) has limitations on the total number of available IP addresses.[2] If it were not for NAT the Internet today would not function for a lack of available addresses.

23) Plaintiffs' witness Linares' declaration, at ¶ 12, states:

"This is analogous to the telephone system where each location has a unique number. For example, in a particular home, there may be three or four different telephones, but only one call can be placed at a time to or from that home."

---

private IP networks that use unregistered IP addresses to connect to the Internet. NAT operates on a router, usually connecting two networks together, and translates the private (not globally unique) addresses in the internal network into legal addresses, before packets are forwarded to another network. As part of this capability, NAT can be configured to advertise only one address for the entire network to the outside world. This provides additional security by effectively hiding the entire internal network behind that address."

[2]American Registry for Internet Numbers (ARIN) submitted as ***Exhibit 8*** description of IPv4 versus IPv6 (**http://www.arin.net/media/fact_sheets/IPv4_IPv6.pdf**) "IPv4 was the first version of Internet Protocol to be widely used, and still accounts for most of today's Internet traffic. There are just over 4 billion IPv4 addresses. While that is a lot of IP addresses, it is not enough to last forever."

Does Exhibit 3

a). In my opinion, this is misleading because Mr. Linares' analogy does not fit the facts of the case as reflected by Plaintiffs' Complaint with Exhibit A and Plaintiffs' subpoena to OSU with Exhibit A.

b). The reasons for my opinion include but are not limited to:
A telephone network is a circuit-switched network. It dynamically creates and removes a circuit or end-to-end link between the two devices that wish to communicate. That is precisely why there may be three or four different phones, but only one call can be placed for a given point in time in the Plaintiff's analogy.

The Internet (which the Plaintiffs claim is the delivery mechanism in this case) is not a circuit-switch network. Instead, it is a packet-switched network.[3] In such a network individual packets are created by the end point devices and deposited onto the network with destination information. Control devices within the network can then decide which path the individual packets will take across the network. Not all packets of a given communication stream will necessarily take the same path. As such in a given network, there can be many simultaneous communication streams that are presented through a single control point and all logged as coming from a single IP address.

This refutes the statements of Plaintiffs' witness Mr. Linares that there cannot be multiple devices in homes and dorms communicating simultaneously. There are in fact, an increasing number of devices that are utilizing wireless technology to bring greater connectivity into the home, the dorm an apartment and other locations. This creates even greater demand for wireless networking, and therefore greater risk for network compromise – and accompanying

---

[3] ***Exhibit 9*** "History of Communications Infrastructures" by Randy H. Katz, Ph.D., Professor of Computer Science, University of Berkley, pg.2, ¶1 (http://bnrg.cs.berkeley.edu/~randy/Courses/CS39C.S97/Internet/Internet.html) ("Telephone system is centralized switching architecture; rigid concept of connection or 'circuit' that must be established between the parties of a communications. If a pathway or switch is broken (or destroyed) during a connection, the path will be broken and the communications will fail. Unacceptable in a survivable system. Replace centralized switches with large numbers of distributed routers, each with multiple connections to adjacent routers. Messages would be divided into parts (*blocks* or *packets*), routed independently, on a packet by packet basis.").

Does Exhibit 3

difficulty in linking IP addresses to specific individuals or their networks. For example, Strategic Analytics of Boston, MA stated in July 2006 that they expect 950 million wireless devices, including games consoles, wireless MP3 players, and mobile phones to be sold by 2010.[4]

I have prepared a diagram marked ***Exhibit 10*** to show that many internal devices can hide behind one external IP address. My diagram depicts the inaccuracies of Mr. Linares' statements.

24) Plaintiffs' witness Linares' declaration, at ¶ 12, states:

"The network provider maintains a log of IP address allocations."

a. In my opinion this statement assumes facts without any supporting evidence.

b. The reasons for my opinion include but are not limited to:

Network providers in a network of networks may maintain logs of IP allocations. However, they do not know the end-point IP address of devices that are depositing packets into their networks. A consumer may install a router for a home network. A student may install a wireless router in his or her dorm room the network provider will know the IP address they have assigned to the router the consumer or student installed. However, the network provider will have no mechanism for identifying the IP addresses for any devices behind that router because of the packet-switched nature of the Internet. Additionally, many consumer/ student oriented control devices (routers, wireless access points) in their default configurations do not log the IP addresses they dynamically assign to end point devices. Therefore even a review of the final network control device cannot provide uniquely-identifiable information about end points once a given communication stream has ended.

25) Plaintiffs' witness Linares' declaration, at ¶ 12, states:

"An IP address can be associated with an organization such as an ISP, business, college, or university, and that organization can identify the P2P network user associated with the specified IP address."

---

[4] ***Exhibit 11***, (http://www.strategyanalytics.com/press/PR00311.htm).

Does Exhibit 3

a. In my opinion, this statement is factually erroneous.

b. The reasons for my opinion include but are not limited to:
On the Internet, network providers are assigned blocks of IP addresses and can, in turn, allocate sub-blocks to their customers who would include businesses, colleges, universities, or other organizations. However, in a packet-switched network, the network providers and even their customers cannot be assured of the unique identity of all devices placing packets on their networks. Control devices can be introduced into sub-networks that mask IP addresses. This is done to allow duplicate IP addresses to exist on a network of networks and still maintain proper routing to end points. The packet switched nature of the communication process means that after a given communication stream is completed, the end points may not necessarily be logged by devices mid-stream. In addition, one end-point will not necessarily be able to know the true location of the other end-point in a given communication stream.

26) Plaintiffs' witness Linares' declaration, at ¶ 13, states:

"Just as any other user on the same P2P networks as these individuals would be able to do, MediaSentry is able to detect the infringement of copyrighted works and identify the user's IP addresses because the P2P software being used by those individuals has file-sharing features enabled."

a. In my opinion, this statement is factually erroneous.

b. The reasons for my opinion include but are not limited to:
The file-sharing features referenced are not sufficient to uniquely identify the device at the end point of a P2P communication stream. As already noted, an IP address may be duplicated on a network of networks such as the Internet. The evidence presented in Plaintiffs' Exhibit A to their Complaint and Plaintiffs' Attachment A to their subpoena to OSU references control node IP addresses of OSU that do not necessarily correspond to the final IP address of the end point device which may or may not have obtained the material in question in this case.

27) Plaintiffs' witness Linares' declaration, at ¶ 14, states:

Does Exhibit 3

"That evidence includes downloaded data files that show for each music file the source IP address, user logs that include a complete listing of all files in the individual's share folder at the time, and additional data that track the movement of the files through the Internet."

a. In my opinion the Plaintiffs' witness Mr. Linares' statements are not supported by current technology and Plaintiffs' factual evidence.

b. The reasons for my opinion include but are not limited to:
There is no evidence in the record presented by the Plaintiffs to show how a sample downloaded file obtained by MediaSentry can be traced back to unnamed and unidentified individuals. Music files, in this case (most likely MP3 files), are not encoded with the IP address of the last system that held the file. Assuming that the Plaintiffs and their agents could provide metadata identifying an IP address of the alleged users, that is not sufficient to identify who shared the file based on the fact that the IP address reported would be most likely a non-public non-routable IP address; i.e., 192.168.1.X, 192.168.2.X, etc.

28) Plaintiffs' witness Linares' declaration, at ¶ 16, states:

"Once provided with the IP address, plus the date and time of the infringing activity, the infringer's ISP quickly and easily can identify the computer from which the infringement occurred (and the name and address of the subscriber that controls that computer), sometimes within a matter of minutes."

a. In my opinion Mr.Linares' makes misleading statements and suggests precision where precision does not exist.

b. The reasons for my opinion include but are not limited to:
An ISP (internet service provider) is a network aggregator in a network of networks model such as the Internet. OSU is the ISP in this case. OSU, as an ISP, can provide a connection between a given IP address and timestamp combination with an individual account if their logging capabilities are enabled. However, this does not assure that the individual identified is the originator of a given series of packets associated with a targeted communication stream.

Does Exhibit 3

In fact, there are many opportunities with existing networking technology deployed on the Internet today to inject a communication stream behind an individual's ISP account without their knowledge. Two examples are: (1) wireless networks that present opportunity to join a sub-network without the owner's knowledge; and, (2) malicious code that can be introduced on a computer to provide remote control capabilities. Botnet, Trojan, and Back Door are examples of malicious codes that can take over the victim's machine without their knowledge or permission.

My reasons set forth in the above paragraphs 21 through 27 further supports my opinions.

As wireless networking technologies have proliferated, there are increasing opportunities to use unsuspecting individual's networks as injection points for unauthorized activities. In fact, many wireless control points are sold with "open" or insecure default configurations. Vendors are motivated to sell products that are easy to install and configure. Configuring secure networks can be complicated and require knowledge many vendors do not wish to require of their customers.

An example of the dangers of open networks is the case of Walter Nowakoski. Nowakoski connected to unsecured home networks and used the bandwidth via unencrypted wireless networks to download child pornography.[5] This is an example of criminals using networks of others to commit crimes so that the innocent are victims twice – once for the theft of their own network resource and then when they are wrongly accused for the illegal activity.

An additional significant threat is malicious code. It is so much of a threat that the antivirus industry reported total revenues of $4 billion in 2005, a 13.6 percent increase over the prior year.[6] Individuals, companies, and universities must defend against malicious threats to the integrity of their computing devices and networks. The fact that there is such a large and fast-growing business devoted to defending networks suggests that there is not a sufficient solution to defeat unauthorized packet injection without significant sophistication.

---

5 ***Exhibit 6 (*** **http://www.ctv.ca/servlet/ArticleNews/story/CTVNews /1069439746264 64848946).**

6 ***Exhibit 7*** Gartner study June 21, 2006 (http://www.gartner.com/press **releases/asset_ 154006_11.html).**

Does Exhibit 3

Conclusion

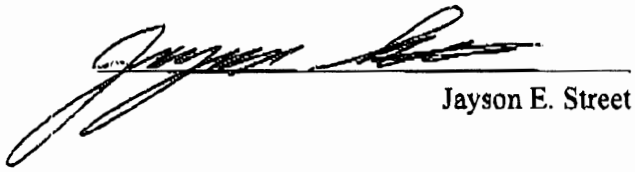
In summary, the claim that an IP address uniquely identifies an individual is an oversimplification and illustrates the Plaintiffs' attempt to use technical terms to assign blame without evidence sufficient to identify the alleged file sharer.

OSU uses its own control point which it hides many devices behind one external internet IP address which then has individual computers or control points (routers, wireless routers, etc.).

Plaintiffs' suggest that being assigned a given IP address at a given time is sufficient to assign liability for all activity originating from that network. However, in the consumer technology market today, there is not sufficient capability to prove such activity and to support Plaintiffs' suggestion. As such, the Plaintiffs have not shown that the IP addresses presented in Plaintiffs' Exhibit A to their Complaint and Plaintiffs' Attachment A to their subpoena to OSU actually correspond to specific individuals or even specific individual devices.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Executed on this 6 day of August, 2007 in Las Vegas, Nevada.



Jayson E. Street

Does Exhibit 3