

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

Arista Records, LLC, a Delaware limited liability company, et al.,	§	
Plaintiffs,	§	
vs.	§	Case No. CIV-07-568-R
Does 1-11,	§	
Defendants.	§	

**DEFENDANT(S) DOE(S) BRIEF IN SUPPORT OF
MOTION TO QUASH PLAINTIFFS’ SUBPOENA DIRECTED TO NON-PARTY
OKLAHOMA STATE UNIVERSITY**

Defendant(s)Doe(s)(hereinafter “Does”) respectfully submit a memorandum of authorities with supporting evidence to support an Order vacating the Court’s May 18, 2007 Order granting the Plaintiffs’ *Ex Parte* Application for Leave to Take Immediate Discovery; and, quashing Plaintiffs’ subpoena dated May 25, 2007 issued to non-party Oklahoma State University (hereinafter “OSU”). 20 U.S.C. §1232h (Protection of pupil rights)(Family Educational Rights & Privacy Act of 1974, as amended); 20 U.S.C. §1232g (Family education and privacy rights);17 U.S.C. § 512(h)(subpoena supported by declaration); Fed. R.Civ. P. 26; Fed. R. Civ. P. 45 c) (3).

I. Limited Appearance Without Waiver of Challenges to Jurisdiction And Venue

Plaintiffs have not caused any summonses to be issued by the Court Clerk and have not served any of the Defendant Doe(s) with the complaint and summonses as reflected by the Court’s record.

Various Doe(s) specially appear for the limited purpose of this motion. Various Does reserve all rights to challenge the Complaint, jurisdiction, venue, and to assert any and all defenses available to them in accordance with the Federal Rules of Civil Procedure.

II. November 17, 2004 General Order, *In re Cases Filed by Recording Companies*

The Court should dismiss without prejudice Plaintiffs' complaint filed in this case based upon principles of collateral estoppel, preclusion and *res judicata*. The Court should give effect to and enforce the November 17, 2004 General Order entered *sua sponte* by the Honorable U.S. District Judge Sam Sparks and the Honorable U.S. District Judge Lee Yeakel, *In re: Cases Filed by Recording Companies*, in the U.S. District Court for the Western District of Texas, Austin Division, wherein the Court *sua sponte* held that joinder of "Does" pursuant to Fed. R. Civ. P. 20(a) was not proper because the alleged copyright claim against each defendant Doe is individual, based on individual acts of each defendant, and, if proven, will result in unique damage claims. *Does' Attachment 1* (11-17-2004 General Order, at 1-2 and attached list of Plaintiffs' cases). The Court also relied upon practical reasons that considerable loss of revenue to the public coffers arises from Plaintiffs improper joinder of Does. "Plaintiffs are ordered to file any future cases of this nature against one defendant at a time, and may not join defendants for their convenience." *Does' Attachment 1*. In the case at bar, Plaintiffs' complaint clearly violates the letter and spirit of the *sua sponte* order filed as *Does' Attachment 1*.

III. Protection of Pupil Rights And the Copyright Act

The Family Educational Rights & Privacy Act of 1974 ("FERPA"), 20 U.S.C. § 1232h (Protection of pupil rights), provides as follows:

- (a) Inspection of instructional materials by parents or guardians
All instructional materials, including teacher's manuals, films, tapes, or other supplementary material which will be used in connection with any survey, analysis, or evaluation as part of any applicable program shall be available for inspection by the parents or guardians of the children.
- (b) Limits on survey, analysis, or evaluations
No student shall be required, as part of any applicable program, to submit to a survey, analysis, or evaluation *that reveals information concerning--*
 - (1) political affiliations or beliefs of the student or the student's parent;

(2) mental or psychological problems of the student or the student's family;
(3) sex behavior or attitudes;
(4) **illegal, anti-social, self-incriminating, or demeaning behavior;**
(5) critical appraisals of other individuals with whom respondents have close family relationships;
(6) **legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers;**
(7) religious practices, affiliations, or beliefs of the student or student's parent; or
(8) income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program),
without the prior consent of the student (if the student is an adult or emancipated minor), or in the case of an unemancipated minor, **without the prior written consent of the parent.**
20 U.S.C. §1232h(2007)(emphasis added).

Under FERPA, personal information means individually identifiable information including a student or parent's first and last name, a home or other physical address (including street name and the name of the city or town; a telephone number, or social security number. 20 U.S.C. § 1232h (c)(6) (2007). *See*, 5-18-07 Order, Doc. 8, (Plaintiffs seek this information from non-party OSU).

(Various) Does do not consent to disclosures by OSU. Plaintiffs attempt to circumvent the provisions of FERPA as to OSU students.

The Copyright Act, 17 U.S.C. § 512(h)(2007), allows for a subpoena to be issued for identification of an alleged infringer and requires, in pertinent part: "**a sworn declaration** to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that the information may only be used for the purposed of protecting rights under the Copyright Act. *See*, 17 U.S.C. § 512(i) ("As used in this subsection, the term 'standard technical measures' means technical measures that are used by copyright owners to identify or protect copyrighted works and--(A) have been **developed pursuant to a broad consensus** of copyright owners and service providers in an **open, fair, voluntary, multi-industry standards process**; (B) are **available to any person on reasonable and nondiscriminatory terms**; and (C) do not impose substantial costs on service providers or substantial burdens on their systems or

networks.”)(emphasis added). 17 U.S.C. § 505 (2007)(prevailing party remedies for non-infringement); 17U.S.C. § 512 (f)(2007)(any person who knowingly materially misrepresents under Section 512 that material or activity is infringing, or that material or activity was removed or disabled by mistake or misidentification shall be liable for damages, including costs and attorneys’ fees.).

IV. Plaintiffs’ *Ex Parte* Application [Docket No. 6] and Declaration of Carlos Linares [Doc. 7-2]

A. The *Ex Parte* Order Granting Expedited Discovery Pursuant to 47 U.S.C. §551(c)(2)(B) and Fed. R. Civ. P. 26 & 45 Should Be Vacated And Plaintiffs’ Subpoena Served on Non-Party OSU Should be Quashed Because Plaintiffs Have Failed to Make a Prima Facie Showing of Copyright Infringement

Plaintiffs’ subpoena served on OSU seeks:

Information, including names, school and permanent addresses and telephone numbers, e-mail addresses, and Media Access Control addresses, sufficient to identify the alleged infringers of copyrighted sound recordings listed by IP address in Attachment A to this Subpoena. ***Does Exhibit 2*** (with attached list).

The subpoena seeks identification of certain individual users of internet services provided by OSU to students, faculty, and other employees on the grounds that the individual users of internet services infringed Plaintiffs’ copyrights by storing files on their computers while connected to the internet without sufficient protection to prevent third parties from accessing those music files and copying them. OSU is an internet service provider - “ISP” for employees, students, visitors, and faculty. Plaintiffs are unable to identify any individual computer from which any alleged infringement of their copyrighted music occurred.

The only copying alleged was conducted by Plaintiffs’ agent, who apparently had permission to copy the files. Plaintiffs’ Memorandum of Law, Doc. No. 7, pgs. 2-3 (citations omitted); Linares’

Declaration.

Plaintiffs do not allege [and cannot allege/prove] that: (1) actual copyright infringement by any individual users of OSU's ISP internet services whose identities are sought by Plaintiffs' subpoena; (2) any individual users of OSU's ISP invited anyone to copy Plaintiffs' music files; (3) any individual user of OSU's ISP were even aware that music files could be copied by third parties such as Plaintiffs' agents; (4) individual users of OSU's ISP have a duty for to protect Plaintiffs' music files from copying by third parties over the internet.

Plaintiffs' declarant Linares does not allege any actual instances of illegal downloading of copyrighted files onto anyone's computers by any of the individuals referred to as "Does." No showing of instances of actual uploading of copyrighted files from any Doe computer to the public is made *but for* the Plaintiffs and their agent(s). No showing is made by Plaintiffs that their representatives and agents are licensed (in Oklahoma or otherwise) to engage in the tasks set forth in the Linares declaration. Moreover, Plaintiffs mistakenly suggest having copyrighted music files on an individual computer or on an assigned folder on OSU's server is "distribution" of copyrighted music. A copyright owner's exclusive right to distribution is set forth in 17 U.S.C. § 109 of the Copyright Act and prohibits a person who possesses a copy of a computer program or of music from distributing for the purpose of direct or indirect commercial advantage. Plaintiffs do not contend that any Doe received a commercial advantage by alleging storing copyrighted files. Plaintiffs theory of copyright infringement has been considered and rejected in prior cases. *National Car Rental Sys. v. Computer Assoc.*, 991 F.2d 426, 434 (8th Cir. 1993)(infringement of distribution rights requires actual dissemination); *Obolensky v. G.P. Putnam's Sons*, 628 F.Supp. 1552, 1555-56 (S.D.N.Y.)(no infringement on copyright owner's right of book distribution by listing the book in

a publication). *Arista Records, Inc. v. MP3 Board, Inc.* 2002 U.S. Dist. Lexis 16165 at 13-14 (S.D. N.Y. 8-29-02).

B. Plaintiffs' Evidence - Linares' Declaration, Plaintiffs' Exhibits and Complaint

A motion for expedited discovery to obtain the identity of John Doe defendant should be denied when plaintiff fails to make an evidentiary showing of each element of their *prima facie* case. *Dendrite Int'l, Inc. v. Doe No. 3*, 342 N.J. Super. 134, 141, 157-159, 775 A.2d 756, 760, 771-72 (N.J. App. 2001)(denial of motion for expedited discovery to obtain identity of Doe was affirmed on appeal because of failure to make evidentiary showing of each element of prima facie case.).

Doe(s) submit the declaration of Jayson E. Street, *Does Exhibit 3* and his supporting evidence, *Does Exhibits 4-11*, to support the relief sought by the Does to reflect significant deficiencies in recitations made by Plaintiffs' declarant Carlos Linares, *Does Exhibit 12*. Mr. Street has addressed the most fundamental and problematic statements made by Linares as they relate to the Does. *Does Exhibit 3*, at 8, ¶ 20.

Plaintiffs 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. *Does Exhibit 3*, at 1-15; 15.

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.

Does Exhibit 3, at 15 (emphasis added).

The Linares declaration is technologically and factually flawed.¹ Linares' declaration, at 5, ¶ 12 recites:

“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.” *Does Exhibit 12*.

This statement is factually erroneous because:

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).

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.

Does Exhibit 3, (Declaration of J. Street) at 8, ¶21.²

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.” *Does Exhibit 12* at 5. This statement is factually erroneous because:

¹The Court's May 18, 2007 Order, Doc. 8, expressly relies upon the Plaintiffs' Declaration of Carlos Linares. Plaintiffs provide only dynamic IP addresses to support allegations against Does. See *Does' Exhibit 1*, Plaintiffs' Complaint, Exhibit A (list of alleged Doe 1-11 with an alleged IP address for each Doe and alleged IP Address with list of alleged songs); See also *Does' Exhibit 2*, Plaintiffs' subpoena dated May 25, 2007 with Attachment A (Plaintiffs' list of Doe(s) 1-11 with IP addresses).

² Street Declaration, at 8, fn. 1 (citing to *Does Exhibit 5* Cisco, Inc. Frequently Asked Questions) . . . (“Network Address Translation (NAT) is designed for IP address simplification and conservation. It enables 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.”).

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. If it were not for NAT the Internet today would not function for a lack of available addresses.

Does Exhibit 3 (Declar. J. Street), at 9, ¶ 22 (emphasis added).

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.”

Does Exhibit 12, Linares at 5 (emphasis added),

In Mr. Street's opinion, this statement 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. The reasons for Mr. Street's opinion are:

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.*(fn.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.

Does Exhibit 3, J. Street declaration at 9-10 (emphasis added).

Mr. Street further opines:

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 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. (citation to **Does Exhibit 9** with quotations omitted).

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.

Does Exhibit 3, J. Street declaration at **10** (emphasis added); **Does Exhibit 9 & 10**.

Linares' declaration, at ¶ 12, states "The network provider maintains a log of IP address allocations." **Does Exhibit 12** at 5. Mr. Street also challenges this statement:

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.*

Does' Exhibit 3, Declar. J. Street, at 11, ¶ 24 (emphasis added).

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." **Does Exhibit 12** at 5.

This statement is factually erroneous because:

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.

Does Exhibit 3, J. Street Declar. at 11-12, ¶ 25 (emphasis added).

Moreover, 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.” *Does Exhibit 12* at 5-6.

This is factually erroneous because:

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. Does Exhibit 3, J. Street Declar, at 12, ¶ 26 (emphasis added).

Plaintiffs' Declarant Linares' at ¶ 14, states:

“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.” *Does Exhibit 12* at 6.

Mr. Linares' statements are not supported by current technology and Plaintiffs' facts because:

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.*

Does Exhibit 3, J. Street Declar. at 12-13, ¶ 27 (emphasis added).

Plaintiffs Declarant Linares, *Does Exhibit 12 at 7, ¶ 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.”

Mr.Linares’ makes misleading statements and suggests precision where precision does not exist.

Does Exhibit 3, J. Street Declar, at 13.

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.**

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.

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.

Does Exhibit 3, J. Street Declar. at 13-14, ¶ 28 (emphasis added); *See Does Exhibits 6-7.*

Mr. Street identifies examples of the dangers of open networks to show 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. *Does Exhibit 3*, at 14; *Does Exhibit 6* (Nowakoski connected to unsecured home networks and used the bandwidth

via unencrypted wireless networks to download child pornography.) **Does Exhibit 7** (significant threat of malicious codes).

The use of unidentified “John Doe” defendants in complaints and expedited discovery obtained *ex parte* is disfavored by Courts. *Strauss v. City of Chicago*, 760 F.2d 765, 770 n.6 (7th Cir. 1985); *In re Ticketplanet.com*, 313 B.R. 46, 55 n. 4 (Bankr. S.D.N.Y. 2004); *Petway v. City of New York*, 2005 WL 2137805 at 4 (E.D. N.Y. 9-2-2005).

In a copyright infringement case, a plaintiff who seeks expedited discovery to uncover the identity of an unknown “John Doe” defendant must make a “concrete showing of a prima facie infringement.” *Sony Music Entertainment Inc. v. Does 1-40*, 326 F.Supp.2d 556, 564-65 (S.D.N.Y. 2004).

Plaintiffs must make an evidentiary showing “that an act giving rise to civil liability actually occurred and that the discovery is aimed at revealing specific identifying features of the person or entity who committed the act” to obtain discovery as to the identity of John Doe defendant. *Columbia Insur. Co. v. Seescandy.com*, 185 F.R.D. 573, 577 (N.D.Cal. 1999). In the case at bar, Plaintiffs have not and cannot make such a showing.

If Internet users could be stripped of [the ability to communicate anonymously on the Internet] by a civil subpoena enforced under the liberal rules of civil discovery, this would have **a significant chilling effect** on Internet communications and thus **on basic First Amendment rights**. Therefore, discovery requests seeking to identify anonymous Internet users must be subjected to careful scrutiny by the courts. *Doe v. 2themart.com Inc.*, 140 F.Supp.2d 1088 (W.D. Wash. 2001)(emphasis added). A real evidentiary basis must be demonstrated by a plaintiff seeking discovery to identify a John Doe defendant in order to protect against unjustified invasions of a John

Doe defendant's right of privacy and anonymity. *Highfields Capital Management v. Doe*, 385 F. Supp.2d 969, 970; 975-76 (N.D. Cal. 2005). Plaintiffs must adduce competent evidence which must address all of the inferences of fact which plaintiffs would need to prove in order to prevail under at least one cause of action asserted by plaintiffs. *Highfields*, at 975-976 ("In other words, the evidence that plaintiff adduces must, if unrebutted, tend to support a finding of each fact that is essential to a given cause of action.").

Additionally, Doe(s) also file herewith for judicial notice to be taken of the declarations of Azer Bestavros, Doc. No. 110, (***Does Exhibit 13***) and Jesse Robert Stengel, Doc. 118, (***Does Exhibit 14***) filed in *Arista Records, LLC. et. al. v. Does 1-21*, Case No. Civ-04-12434-NG (consolidated with Case No. Civ-07-10834-NG) in July 2007 to support Does' motion to quash plaintiffs' *ex parte* subpoena issued to Boston University.).

V. Conclusion

The Court should grant the Does any and all relief the Court deems appropriate, including but not limited to dismissal of Plaintiffs' Complaint against the Does, vacatur of the Court's expedited discovery order, quashing of plaintiffs' subpoena to non-party OSU, and award Does their attorneys' fees and costs under the authorities relied upon by the Defendant(s) Does.

Respectfully submitted,
s/ Marilyn D. Barringer-Thomson
Marilyn D. Barringer-Thomson
OBA# 11057
Post Office Box 54444
Oklahoma City, Oklahoma 73154
(405) 840-3101 Telephone
(405) 842-3843 Telecopier
barringerlawfirm@sbcglobal.net
and

Warren W. Henson, III OBA# 13084
4901 Richmond Square, Suite 104
Oklahoma City, Oklahoma 73118
(405) 840-3889 Telephone
(405) 843-0322 Telecopier
Counsel for Defendant Doe(s)

CERTIFICATE OF SERVICE

This is to certify that on this 6th day of August, I electronically transmitted the above and forgoing to the Clerk of the Court using the ECF System for filing. Based on the electronic records current on file, the Clerk of the Court will transmit a Notice of Electronic Filing to the all ECF registrants in this case:

Lisa R. Hemphill
GARDERE WYNNE SEWELL
LLP
1601 Elm Street, Suite
3000
Dallas, Texas 75201-4761
Telephone: 214-999-4682
Telecopier: 214-999-3682
lhemphill@gardere.com
Counsel for Plaintiffs

Ryan T. Leonard
Leonard Gould & Brown
PLLC
116 East Sheridan, Suite
207
Oklahoma City, OK
73104
Telephone: 405-605-8383
Telecopier: 405-605-8381
leonard@lgblawfirm.com
Counsel for Plaintiffs

Michael Scott Fern
Associate General Counsel
Oklahoma State University
Student Union Building
Oklahoma State University
Stillwater, OK 74078-7044
Telephone: 405-744-6494
Telecopier: 405-744-7998
msfern@okstate.edu

Subpoena Issued to Non-Party
Oklahoma State University by
Plaintiffs

S:/Marilyn D. Barringer-Thomson
Marilyn D. Barringer-Thomson