Expert Report of Chris Beall

UMG Recordings, Inc.
v.
Janne Lanzoni
Case No. 4:08-cv-03025
U.S. District Court – Southern District of Texas

Chris Beall
March 9, 2009

Introduction and Summary of Opinions

1. My name is Chris Beall. I have been engaged by counsel for Janne Lanzoni to offer expert testimony concerning issues relating to the identification of an individual who allegedly downloaded 10 songs via a peer-to-peer file copying network on February 21, 2007, at 12:54:09 EST, as alleged in the complaint filed against Janne Lanzoni in this case. According to the complaint, MediaSentry, Inc. identified ***an individual*** allegedly determined to be Defendant Janne Lanzoni who used Ares on the peer-to-peer network AresWarez at IP address 70.232.28.96 on February 21, 2007, at 12:54:09 EST, to download the 10 songs alleged in the complaint.

2. In my opinion, using an IP address to identify an individual who was allegedly downloading files over the Internet under the circumstances alleged in the complaint is not a reliable methodology for identifying the individual who was actually engaged in the alleged file downloading activities (assuming that such activities actually occurred as alleged), especially under the circumstances of this case where a wireless router was in use at the Lanzoni home to provide Internet access.

3. Even if we assume for the sake of argument that someone used Ares on the peer-to-peer network AresWarez at IP address 70.232.28.96 on February 21, 2007, at 12:54:09 EST, to download 10 songs as alleged in the complaint, this is

insufficient evidence to prove that Defendant Janne Lanzoni was the individual who did so. There are many common scenarios which make it impossible to identify who actually initiated a file download.

4. Based on the evidence available to me, in my opinion, Janne Lanzoni was ***not*** the individual who allegedly used Ares on the peer-to-peer network AresWarez at IP address 70.232.28.96 on February 21, 2007, at 12:54:09 EST, to download 10 songs as alleged in the complaint.

Bases For Opinions

5. According to the Declaration of Janne Lanzoni, dated March 4, 2009, she was at work on February 21, 2007, at 12:54 EST at Carver High School, 2100 S. Victory Drive, Houston, Texas 77088. The complaint alleges that the IP address (70.232.28.96) used by the individual who allegedly downloaded the files was traced back to Janne Lanzoni's home address at 6010 Black Maple Lane, Houston, Texas 77088. If Janne Lanzoni was not at or near her residence at 6010 Black Maple Lane, Houston, Texas 77088 at the time the files were allegedly downloaded, then she could not have been the individual who downloaded the files on the date and time alleged in the complaint.

6. According to the Declaration of Janne Lanzoni, dated March 4, 2009, she had a wireless network in her home on the relevant date alleged in the

complaint. According to her declaration, the wireless network in her home on February 21, 2007, was not secured.

7. An open wireless network using an unsecured wireless router with no encryption at the Lanzoni residence could have been accessed by any nearby computer user with sufficient signal strength to make a connection. Anyone who connected to the wireless network at the Lanzoni home would have appeared to the outside world as having the same IP address that was currently assigned to Janne Lanzoni's wireless router. Assuming that the IP address 70.232.28.96 was the correct IP address that was actually assigned to Janne Lanzoni's wireless router at that point in time, anyone who connected to the wireless network at the Lanzoni home on February 21, 2007, at the time alleged in the complaint would appear to be using that same IP address 70.232.28.96.

8. The surrounding neighborhood for Janne Lanzoni's home address at 6010 Black Maple Lane, Houston, Texas 77088 is shown by Google Earth. Exhibit B, Exhibit C and Exhibit D are various views of the area surrounding the Lanzoni home. Janne Lanzoni lives in a neighborhood where the houses are closely packed together. The minimum separation between the Lanzoni house and the immediately adjacent houses appears to be only a few feet.

9. Exhibit E is a schematic diagram that may be used to describe an average or typical coverage area for a wireless network in the location of the Lanzoni

home. The distance at which someone nearby could have accessed the Lanzoni wireless network may have been increased or extended by the use of a directional or gain antenna to make the connection to the Lanzoni wireless network. Exhibit F is a close up view of the diagram of Exhibit E. In my opinion, the wireless network at the Lanzoni home could have been accessed from a number of nearby locations, including computers located in a neighbor's house or in a vehicle parked on the street.

10. IP addresses that are assigned to an Internet access point are often dynamic (as opposed to static), meaning that every time a particular computer or device signs onto the Internet, it can receive a different IP address than the previous time. Internet service providers often share IP addresses back and forth between separate access points to maximize their availability at any given time.

11. An IP address is not necessarily limited to a single computer or a single user. A group of computers can share the same IP address, and this will occur when a wireless router is used for Internet access via a home wireless network. Any computer connected to the wireless home network that accesses the Internet will share the same IP address through the wireless router. The description in the Brief of Amici Curiae marked as Exhibit G is accurate in this respect.

12. There are a number of common scenarios which make it impossible to identify who actually initiated a file download. For example, the following common scenarios will lead to an incorrect identification of the individual who initiated a file download, under circumstances where the IP address recorded by the Internet service provider will be that of the account holder:

a. A neighbor deliberately accesses the account holder's unsecured wireless router.

b. A neighbor inadvertently accesses the account holder's unsecured wireless router, thinking it is their own wireless router. This happens frequently with popular brands of routers, which are usually left in their default configuration, in situations where the physical setup causes the signal from a neighbor's router to be stronger than the signal from one's own router.

c. A stranger, such as someone parked on the street outside the residence, accesses the account holder's unsecured wireless router. Maps of unsecured wireless access points are published on the Internet, and specialized equipment is sold for use in detecting open access points, including from a moving vehicle.

d. The account holder sells or disposes of a computer, video game console, or other device that was previously connected to their wireless router,

and the purchaser uses the access credentials that are recorded on that device to access the account holder's wireless router.

e. A stranger uses stolen or published access credentials to access the account holder's secured wireless router.

f. A computer on the account holder's network becomes infected with a computer virus or other malicious software that downloads and uploads files without any human intervention.

g. A computer on the account holder's network becomes infected with malicious software that allows it to be controlled by a stranger somewhere on the Internet, and is used for downloading or uploading files.

h. A computer on the account holder's network becomes infected with malicious software that forces it to act as a "hijacked host" or proxy to disguise the IP addresses of other computers that are used for illegal downloads or file sharing.

i. A visitor is given physical access to any computer on the account holder's network.

j. A visitor who uses a network cable to plug in their computer or game console to the account holder's router.

k. A visitor is given the password to use their own computer or video game console to access the account holder's secured wireless router.

l. A visitor accesses the account holder's unsecured wireless router.

m. In each of these scenarios, the IP address that the Internet Service Provider would report as having downloaded a file is the account holder's, but the actual download may have been initiated by an authorized or unauthorized visitor, a neighbor, a nearby stranger, a malicious user elsewhere on the internet, or even a non-human computer virus or other malware. All of these cases are completely indistinguishable by IP address. In some scenarios, the account holder is nothing more than the unknowing victim of access to their Internet account by technically sophisticated criminals.

13. According to the Expert Report of Dr. Yongdae Kim, Ph.D., filed in the case of *Capital Records, Inc., et al. v. Thomas*, "MediaSentry's methods are lacking even the most basis of error control and mitigation procedures." *Id.* at 9-10. If MediaSentry's methods are not reliable, then the unreliability of the Plaintiffs' use of an IP address to identify Janne Lanzoni in this case is further exacerbated.

14. My qualifications are set forth in Exhibit A.

15. I have not testified as an expert at trial or by deposition in any other case within the preceding four years.

16. The information considered in reaching my opinions includes:

a. The information alleged in the complaint.

b. The Declaration of Janne Lanzoni, dated March 4, 2009.

c. The layout and configuration of dwellings and streets in the vicinity of 6010 Black Maple Lane, Houston, Texas 77088 as shown by Google Earth.

d. Information was provided to me that no one was at home at the Lanzoni residence on February 21, 2007, at the time alleged in the complaint. Janne Lanzoni's husband Fred Garcia was at work at Land, Sea and Sky – Texas Nautical Repair, 1925A Richmond Avenue, Houston, Texas 77098, and their two minor children were attending school.

e. Brief of Amici Curiae American Association of Law Libraries, American Civil Liberties Union, ACLU of Oklahoma Foundation, Electronic Frontier Foundation, and Public Citizen, filed in the case of *Capital Records, Inc., et al. v. Foster*, Case No. CIV-04-1569-W (W.D. Okla. Aug. 10, 2006).

f. The Expert Report of Dr. Yongdae Kim, Ph.D., filed in the case of *Capital Records, Inc., et al. v. Thomas*, Case No. 06-1497 (MJD/RLE) (D. Minn. March 2, 2009).

g. The Expert Report of Dr. J.A. Pouwelse, filed in the case of *UMG Recordings, Inc., et al. v. Lindor*, Case No. 05-cv-1095 (E.D.N.Y. February 13, 2008).

Date: March 9, 2009

Chris Beall