IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
SAN ANTONIO DIVISION

WARNER BROS. RECORDS INC., *et al.*,	§	
	§	
Plaintiffs,	§	C.A. NO. 5:06-cv-00615-OLG
	§	
vs.	§	JUDGE ORLANDO GARCIA
	§	
JOSE DUARTE,	§	
	§	
Defendant.	§	
	§	

DECLARATION OF THOMAS CARPENTER

I, Thomas Carpenter, under penalty of perjury, hereby declare and say:

1. I am Director, Data Services for the MediaSentry business unit of SafeNet, Inc ("MediaSentry"). I have personal knowledge of all of the matters discussed in this Declaration.

2. MediaSentry is one of the principal providers of online anti-piracy services worldwide. It specializes in providing services to detect and prevent unauthorized distribution of music, films, software, and other content on the Internet.

3. MediaSentry detected hundreds of digital audio files being distributed for free from a computer connected to the Internet using a specific Internet Protocol ("IP") address on the following occasions:

Date:	IP Address:	No. of Sound Recordings:
June 14, 2004	68.91.88.25	558
June 24, 2004	68.89.131.88	586
June 30, 2004	68.89.136.90	619

4. These IP addresses were assigned to Southwestern Bell Internet Services, Inc. at the dates and times that MediaSentry detected the distribution.

5. On each occasion, MediaSentry recorded screen shots showing the computer distributing hundreds of digital audio files, including Plaintiffs' copyrighted sound recordings, from the computer's shared folder.

6. Each time MediaSentry detected the distribution, the number of sound recordings in the shared folder increased, from 558 sound recordings on June 14, 2004, to 619 sound recordings on June 30, 2004. The increasing number of digital music files in the computer's shared folder indicates that, in addition to the distribution of such from the computer, files were also being copied to the computer's shared folder.

7. On each of the three occasions above that MediaSentry detected the distribution, it downloaded a number of the .MP3 "audio" files that were being distributed for free from the computer's shared folder. The titles of .MP3 files that were downloaded indicated that they were sound recordings whose copyrights are owned by the Plaintiffs in this lawsuit.

8. Copies of the .MP3 "audio" files that were downloaded by MedaSentry were given to the Recording Industry Association of America for review.

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

Executed on this 24th day of January, 2007, in Morristown, NJ.

Thomas Carpenter

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
SAN ANTONIO DIVISION

WARNER BROS. RECORDS INC., *et al.*, Plaintiffs, vs. JOSE DUARTE, Defendant.	§ § § § § § § § § §	C.A. NO. 5:06-cv-00615-OLG JUDGE ORLANDO GARCIA

DECLARATION OF THOMAS CARPENTER

I, Thomas Carpenter, under penalty of perjury, hereby declare and say:

1. I am Director, Data Services for the MediaSentry business unit of SafeNet, Inc ("MediaSentry"). I have personal knowledge of all of the matters discussed in this Declaration.

2. MediaSentry is one of the principal providers of online anti-piracy services worldwide. It specializes in providing services to detect and prevent unauthorized distribution of music, films, software, and other content on the Internet.

3. MediaSentry detected hundreds of digital audio files being distributed for free from a computer connected to the Internet using a specific Internet Protocol ("IP") address on the following occasions:

Date:	IP Address:	No. of Sound Recordings:
June 14, 2004	68.91.88.25	558
June 24, 2004	68.89.131.88	586
June 30, 2004	68.89.136.90	619

4. These IP addresses were assigned to Southwestern Bell Internet Services, Inc. at the dates and times that MediaSentry detected the distribution.

5. On each occasion, MediaSentry recorded screen shots showing the computer distributing hundreds of digital audio files, including Plaintiffs' copyrighted sound recordings, from the computer's shared folder.

6. Each time MediaSentry detected the distribution, the number of sound recordings in the shared folder increased, from 558 sound recordings on June 14, 2004, to 619 sound recordings on June 30, 2004. The increasing number of digital music files in the computer's shared folder indicates that, in addition to the distribution of such from the computer, files were also being copied to the computer's shared folder.

7. On each of the three occasions above that MediaSentry detected the distribution, it downloaded a number of the .MP3 "audio" files that were being distributed for free from the computer's shared folder. The titles of .MP3 files that were downloaded indicated that they were sound recordings whose copyrights are owned by the Plaintiffs in this lawsuit.

8. Copies of the .MP3 "audio" files that were downloaded by MedaSentry were given to the Recording Industry Association of America for review.

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

Executed on this 24th day of January, 2007, in Morristown, NJ.

Thomas Carpenter

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MOTOWN RECORD COMPANY, L.P., et al.,	§	
Plaintiffs	§	
	§	Case No.: 05-CV-5410 (DGT) (RML)
vs.	§	
BRIDGET BYRNES,	§	
Defendant.	§	

DECLARATION OF THOMAS CARPENTER

Thomas Carpenter declares as follows under oath and subject to penalty of perjury:

1. I am Director, Data Services for the MediaSentry Managed Services unit of Safenet, Inc. ("MediaSentry"). I have personal knowledge of all of the matters discussed in this Declaration.

2. MediaSentry is devoted to the management and protection of intellectual property rights, and is engaged in, among other things, the investigation and detection of copyright infringement over the internet. MediaSentry has been engaged by the Recording Industry Association of America ("RIAA") on behalf of the Plaintiffs to assist them in locating individuals infringing their copyrights over the internet.

3. MediaSentry's methods for detecting copyright infringement over the internet are a trade secret and constitute confidential commercial information. MediaSentry has invested tens of thousands of man-hours developing its investigative software, tools, and methods of applying its software over the five years of its existence. MediaSentry serves a broad range of customers and its tools and methods for detecting online copyright infringement are its life blood. Because MediaSentry's business depends on its ability to stay one step ahead of the

online infringement community at all times, and to keep competitors from mimicking its proprietary processes, MediaSentry maintains strict confidentiality concerning its business practices, including its proprietary tools and methods for detecting online infringement, and does not share them with anyone outside of MediaSentry except under limited circumstances and then only with strict confidentiality and non-disclosure requirements. MediaSentry also requires all employees with access to such information to maintain strict confidentiality.

4. MediaSentry has made its business information available to litigants only with a Court-approved protective order in place, and has litigated at great expense to prevent the unprotected disclosure of such information, both within and outside the United States. For example, MediaSentry sought and obtained Court protection of its proprietary business information in the Federal Court of Australia in Universal Music Australia Pty Ltd. v. Sharman License Holdings, Ltd., No. NSD110/2004, and has successfully prevented the production of its source code in Altnet, Inc. v. Recording Industry Association of America, No. 04-CV-745, currently pending in the Central District of California.

5. Due to the significant threat imposed by illegal online file sharing, a number of companies are engaged in the same business as MediaSentry and compete directly with MediaSentry for business. MediaSentry's tools and methods for detecting online copyright infringement are not known to the general public and give MediaSentry a business advantage over its competitors. These tools and methods could not be easily duplicated. The disclosure of MediaSentry's proprietary tools and methods for detecting online infringement would allow MediaSentry' competitors to duplicate easily MediaSentry's methods, which would cause MediaSentry to suffer both the loss of value of its trade secrets and the loss of its current competitive advantage.

6. MediaSentry provides infringement detection services not only for the Plaintiffs in the above lawsuit, but for many customers in the recording, motion picture, and other industries. The disclosure of MediaSentry's tools and methods for detecting online infringement would cause significant harm to MediaSentry's other customers by negatively affecting their ability to pursue other infringers and protect their copyrights.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this 23rd day of June 2006 at Morristown, New Jersey

Thomas Carpenter

Jonathan G. Fetterly (State Bar No. 228612)
HOLME ROBERTS & OWEN LLP
777 South Figueroa Street, Suite 2800
Los Angeles, CA 90017-5826
Telephone: (213) 572-4300
Facsimile: (213) 572-4400
E-mail: jon.fetterly@hro.com

Attorney for Plaintiffs
CAPITOL RECORDS, INC.; UMG RECORDINGS, INC.; and SONY BMG MUSIC ENTERTAINMENT

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

WESTERN DIVISION

CAPITOL RECORDS, INC., a Delaware corporation; UMG RECORDINGS, INC., a Delaware corporation; and SONY BMG MUSIC ENTERTAINMENT, a Delaware general partnership,

Plaintiffs,

v.

COLUMBIA DO TRAN,

Defendant.

Case No.: CV 06-6587 GW (Ex)

DECLARATION OF ELIZABETH HARDWICK

I, Elizabeth Hardwick, pursuant to 28 U.S.C. § 1746, declare as follows:

1. I am the Product Manager, Data Services for the MediaSentry Business Unit of Safenet, Inc., formerly MediaSentry, Inc. ("MediaSentry"). I have personal knowledge of all of the matters discussed in this Declaration except as where stated on information and belief. As to such facts, I believe them to be true.

2. MediaSentry is one of the principal providers of online anti-piracy services worldwide. It specializes in providing services to detect and prevent unauthorized distribution of music, films, software, and other content on the Internet.

3. MediaSentry has been engaged by the Recording Industry Association of America ("RIAA") on behalf of the Plaintiffs to assist them in locating individuals infringing their copyrights over peer-to-peer networks and gathering evidence of their infringement. To perform this task, MediaSentry searches peer-to-peer networks for individuals distributing infringing files for download and gathers evidence concerning that infringement.

4. In gathering evidence of infringement, MediaSentry does not do anything that any user of a peer-to-peer network cannot do and does not obtain any information that is not available to anyone who logs onto a peer-to-peer network. Thus, when MediaSentry searches for sound recordings on the peer-to-peer network, views the files that each peer-to-peer user is disseminating to others, obtains the IP address and screen name of each user, and downloads copyrighted works distributed by each user, it is using functionalities that are built into the peer-to-peer protocols that each user has chosen to use to upload (or distribute) and download (or copy) music.

5. MediaSentry searches peer-to-peer networks, looking for users distributing ("uploading") files that appear to be digital copies of sound recordings whose copyrights are owned by the RIAA's member record companies. When MediaSentry finds such a file, it may download the file. As part of that downloading process, MediaSentry, like any other peer-to-peer user, receives basic information about the user

from whom the work is being downloaded. That information includes, among other things, the Internet Protocol ("IP") address of the user.

6. Once connected to the user's computer MediaSentry also seeks to determine what other files the individual is distributing to others for download. I2Hub and other file-copying programs permit users to share all of the files in their shared folders, and they may contain a feature that permits users to browse the entire shared folder of another user. When available, MediaSentry invokes this feature of a peer-to-peer program, just as any other user could do, and is able to determine whether the individual user is merely distributing one or two music files or whether the user is distributing hundreds or even thousands of music files.

7. Again using a feature of the peer-to-peer software available to any user, MediaSentry can then capture a list of all of the files that the user is distributing to others for download. MediaSentry collects this information by capturing as a text file all of the contents of the user's shared directory, such as the names of each file and the size of each file, as well as additional information (called "metadata") about each file. Metadata may include a wide range of information about a file. Metadata, for example, can include information such as identification of the person or group that originally copied the file and began disseminating it unlawfully. MediaSentry does nothing to create this text file; it exists on the user's hard drive.

8. MediaSentry's process for identifying potential infringers and gathering evidence of infringement has multiple fail-safes to ensure that the information gathered is accurate. MediaSentry takes numerous steps to check and double-check the IP address of the potential infringer to prevent misidentification.

9. MediaSentry followed the procedures outlined above with respect to the evidence that it gathered in this case. Specifically, on September 8, 2005 at approximately 6:32 A.M. EDT, MediaSentry detected the username "[ucsd]kongsta" logged into the I2Hub file-sharing network at IP address 137.110.192.19. Attached as

Exhibit 1 to this Declaration is a true and correct copy of the text file captured by MediaSentry on January 30, 2006 showing the list of files that the computer connected to I2Hub with the IP address of 137.110.192.19 was distributing under the username ""“[ucsd]kongsta” to others for download.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this 14th day of November, 2007.

Elizabeth Hardwick

Elizabeth Hardwick

Ira M. Schwartz (State Bar No. 010448)
Michael A. Cordier (State Bar No. 014378)
DECONCINI MCDONALD YETWIN & LACY, P.C.
7310 North 16th Street, Suite 330
Phoenix, AZ 85020
Telephone: (602) 282-0500
Facsimile: (602) 282-0520
ischwartz@dmylphx.com
mcordier@dmylphx.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

DISTRICT OF ARIZONA

Atlantic Recording Corporation, et al., Plaintiffs, vs. Pamela And Jeffrey Howell, Defendants.	Case No.: 2:06-cv-02076-PHX-NVW **DECLARATION OF ELIZABETH HARDWICK**

I, Elizabeth Hardwick, pursuant to 28 U.S.C. § 1746, declare as follows:

1. I am the Product Manager, Data Services for the MediaSentry business unit of Safenet, Inc., formerly MediaSentry, Inc. ("MediaSentry"). I have personal knowledge of all of the matters discussed in this Declaration except as where stated on information and belief. As to such facts, I believe them to be true.

2. MediaSentry is one of the principal providers of online anti-piracy services worldwide. It specializes in providing services to detect and prevent unauthorized distribution of music, films, software, and other content on the Internet.

3. MediaSentry has been engaged by the Recording Industry Association of America ("RIAA") on behalf of the Plaintiffs to assist them in locating individuals infringing their copyrights over peer-to-peer networks and

gathering evidence of their infringement. To perform this task, MediaSentry searches peer-to-peer networks for individuals distributing infringing files for download and gathers evidence concerning that infringement.

4. In gathering evidence of infringement, MediaSentry does not do anything that any user of a peer-to-peer network cannot do and does not obtain any information that is not available to anyone who logs onto a peer-to-peer network. Thus, when MediaSentry searches for sound recordings on the peer-to-peer network, views the files that each peer-to-peer user is disseminating to others, obtains the IP address and screen name of each user, and downloads copyrighted works distributed by each user, it is using functionalities that are built into the peer-to-peer protocols that each user has chosen to use to upload (or distribute) and download (or copy) music.

5. MediaSentry searches peer-to-peer networks, looking for users distributing ("uploading") files that appear to be digital copies of sound recordings whose copyrights are owned by the RIAA's member record companies. When MediaSentry finds such a file, it may download the file. As part of that downloading process, MediaSentry, like any other peer-to-peer user, receives basic information about the user from whom the work is being downloaded. That information includes, among other things, the Internet Protocol ("IP") address of the user.

6. Once connected to the user's computer MediaSentry also seeks to determine what other files the individual is distributing to others for download. KaZaA and other file-copying programs permit users to share all of the files in their shared folders, and they may contain a feature that permits users to browse the entire shared folder of another user. When available, MediaSentry invokes this feature of a peer-to-peer program, just as any other user could do, and is able to

determine whether the individual user is merely distributing one or two music files or whether the user is distributing hundreds or even thousands of music files.

7. Again using a feature of the peer-to-peer software available to any user, MediaSentry can then capture a list of all of the files that the user is distributing to others for download. MediaSentry collects this information in two forms. First, MediaSentry takes screen shots, which are actual pictures of the screens that MediaSentry or any other user of the peer-to-peer network can see when reviewing the files being distributed. Second, MediaSentry captures as a text file all of the contents of the user's shared directory, such as the names of each file and the size of each file, as well as additional information (called "metadata") about each file. Metadata may include a wide range of information about a file. Metadata, for example, can include information such as identification of the person or group that originally copied the file and began disseminating it unlawfully. MediaSentry does nothing to create this text file; it exists on the user's hard drive.

8. MediaSentry's process for identifying potential infringers and gathering evidence of infringement has multiple fail-safes to ensure that the information gathered is accurate. MediaSentry takes numerous steps to check and double-check the IP address of the potential infringer to prevent misidentification.

9. MediaSentry followed the procedures outlined above with respect to the evidence that it gathered in this case. Specifically, on January 30, 2006 at approximately 1:52 A.M. EDT, MediaSentry detected the username "jeepkiller@KaZaA" logged into the KaZaA file-sharing network at IP address 68.110.64.47. Attached as Exhibit 10 to Plaintiffs' Statement Of Facts In Support Of Motion For Summary Judgment is a true and correct copy of a compilation of screen shots captured by MediaSentry on January 30, 2006 showing the list of files

that the computer connected to KaZaA with the IP address of 68.110.64.47 was distributing under the username "jeepkiller@KaZaA" to others for download.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this 5th day of July 2007.

Elizabeth Hardwick

Elizabeth Hardwick

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF LOUISIANA
LAFAYETTE DIVISION

WARNER BROS. RECORDS INC., a Delaware corporation; UMG RECORDINGS, INC., a Delaware corporation; SONY BMG MUSIC ENTERTAINMENT, a Delaware general partnership; ARISTA RECORDS LLC, a Delaware limited liability company; and BMG MUSIC, a New York general partnership,	CIVIL ACTION NO. 07-1280 JUDGE Tucker L. Melancon MAGISTRATE JUDGE Methvin
Plaintiffs,	
v.	
JAMES VENTRESS LEWIS (AKA JAMES V. LEWIS, JR.),	
Defendant.	

DECLARATION OF ELIZABETH HARDWICK

I, Elizabeth Hardwick, pursuant to 28 U.S.C. § 1746, declare as follows:

1. I am the Product Manager, Data Services for the MediaSentry Business Unit of Safenet, Inc., formerly MediaSentry, Inc. ("MediaSentry"). I have personal knowledge of all of the matters discussed in this Declaration except as where stated on information and belief. As to such facts, I believe them to be true.

2. MediaSentry is one of the principal providers of online anti-piracy services worldwide. It specializes in providing services to detect and prevent unauthorized distribution of music, films, software, and other content on the Internet.

3. MediaSentry has been engaged by the Recording Industry Association of America ("RIAA") on behalf of the Plaintiffs to assist them in locating individuals infringing their copyrights over peer-to-peer networks and gathering evidence of their infringement. To perform

this task, MediaSentry searches peer-to-peer networks for individuals distributing infringing files for download and gathers evidence concerning that infringement.

4. In gathering evidence of infringement, MediaSentry does not do anything that any user of a peer-to-peer network cannot do and does not obtain any information that is not available to anyone who logs onto a peer-to-peer network. Thus, when MediaSentry searches for sound recordings on the peer-to-peer network, views the files that each peer-to-peer user is disseminating to others, obtains the IP address and screen name of each user, and downloads copyrighted works distributed by each user, it is using functionalities that are built into the peer-to-peer protocols that each user has chosen to use to upload (or distribute) and download (or copy) music.

5. MediaSentry searches peer-to-peer networks, looking for users distributing ("uploading") files that appear to be digital copies of sound recordings whose copyrights are owned by the RIAA's member record companies. When MediaSentry finds such a file, it may download the file. As part of that downloading process, MediaSentry, like any other peer-to-peer user, receives basic information about the user from whom the work is being downloaded. That information includes, among other things, the Internet Protocol ("IP") address of the user.

6. Once connected to the user's computer, MediaSentry also seeks to determine what other files the individual is distributing to others for download. KaZaA and other file-copying programs permit users to share all of the files in their shared folders, and they may contain a feature that permits users to browse the entire shared folder of another user. When available, MediaSentry invokes this feature of a peer-to-peer program, just as any other user could do, and is able to determine whether the individual user is merely distributing one or two music files or whether the user is distributing hundreds or even thousands of music files.

7. Again using a feature of the peer-to-peer software available to any user, MediaSentry can then capture a list of all of the files that the user is distributing to others for download. MediaSentry collects this information in two forms. First, MediaSentry takes screen shots, which are actual pictures of the screens that MediaSentry or any other user of the peer-to-peer network can see when reviewing the files being distributed. Second, MediaSentry captures as a text file all of the contents of the user's shared directory, such as the names of each file and the size of each file, as well as additional information (called "metadata") about each file. Metadata may include a wide range of information about a file. Metadata, for example, can include information such as identification of the person or group that originally copied the file and began disseminating it unlawfully. MediaSentry does nothing to create this text file; it exists on the user's hard drive and is distributed by the user to anyone to whom the user distributes files.

8. MediaSentry's process for identifying potential infringers and gathering evidence of infringement has multiple fail-safes to ensure that the information gathered is accurate. MediaSentry takes numerous steps to check and double-check the IP address of the potential infringer.

9. MediaSentry followed the procedures outlined above with respect to the evidence that it gathered in this case. Specifically, on June 13, 2005, at approximately 9:41 p.m., MediaSentry detected the username "LilJames@KaZaA" logged into the KaZaA file-sharing service at IP address 68.191.83.124. Attached as Exhibit B to Plaintiffs' Complaint is a true and correct copy of a compilation of screen shots captured by MediaSentry on June 13, 2005 showing the list of files, including digital music files, that the computer connected to KaZaA with the IP address of 68.191.83.124 was distributing, for free, under the username "LilJames@KaZaA" to others for download. MediaSentry also downloaded a sampling of the

sound recordings that this individual was distributing to other users. A list of five such sound recordings downloaded by MediaSentry from the KaZaA user LilJames@KaZaA connected to the Internet at IP address 68.191.83.124 on June 13, 2005, at approximately 9:41 p.m. is attached as Exhibit A to Plaintiffs' Complaint.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this 24th day of January, 2008.

Elizabeth Hardwick

Elizabeth Hardwick

UNITED STATES DISTRICT COURT

DISTRICT OF MASSACHUSETTS

CAPITOL RECORDS, INC. et al.,
Plaintiffs,

v.

NOOR ALAUJAN,
Defendant.

Civ. Act. No. 03-cv-11661-NG
(LEAD DOCKET NUMBER)

SONY BMG MUSIC ENTERTAINMENT
et al., Plaintiffs,

v.
JOEL TENENBAUM,

Defendants.

Civ. Act. No 07-cv-11446-NG
(ORIGINAL DOCKET NUMBER)

DECLARATION OF ELIZABETH HARDWICK

I, Elizabeth Hardwick, pursuant to 28 U.S.C. § 1746, declare as follows:

1. I am the Product Manager, Data Services for the MediaSentry Business Unit of Safenet, Inc., formerly MediaSentry, Inc. ("MediaSentry"). I have personal knowledge of all of the matters discussed in this Declaration except as where stated on information and belief. As to such facts, I believe them to be true.

2. MediaSentry is one of the principal providers of online anti-piracy services worldwide. It specializes in providing services to detect and prevent unauthorized distribution of music, films, software, and other content on the Internet.

3. MediaSentry has been engaged by the Recording Industry Association of America ("RIAA") on behalf of the Plaintiffs to assist them in locating individuals infringing their copyrights over peer-to-peer networks and gathering evidence of their infringement. To perform this task, MediaSentry searches peer-to-peer networks for individuals distributing infringing files for download and gathers evidence concerning that infringement.

4. In gathering evidence of infringement, MediaSentry does not do anything that any user of a peer-to-peer network cannot do and does not obtain any information that is not available to anyone who logs onto a peer-to-peer network. Thus, when MediaSentry searches for sound recordings on the peer-to-peer network, views the files that each peer-to-peer user is disseminating to others, obtains the IP address and screen name of each user, and downloads copyrighted works distributed by each user, it is using functionalities that are built into the peer-to-peer protocols that each user has chosen to use to upload (or distribute) and download (or copy) music.

5. MediaSentry searches peer-to-peer networks, looking for users distributing ("uploading") files that appear to be digital copies of sound recordings whose copyrights are owned by the RIAA's member record companies. When MediaSentry finds such a file, it may download the file. As part of that downloading process, MediaSentry, like any other peer-to-peer user, receives basic information about the user from whom the work is being downloaded. That information includes, among other things, the Internet Protocol ("IP") address of the user.

6. Once connected to the user's computer MediaSentry also seeks to determine what other files the individual is distributing to others for download. KaZaA and other file-copying programs permit users to share all of the files in their shared folders, and they may contain a feature that permits users to browse the entire shared folder of another user. When available,

MediaSentry invokes this feature of a peer-to-peer program, just as any other user could do, and is able to determine whether the individual user is merely distributing one or two music files or whether the user is distributing hundreds or even thousands of music files.

7. Again using a feature of the peer-to-peer software available to any user, MediaSentry can then capture a list of all of the files that the user is distributing to others for download. MediaSentry collects this information in two forms. First, MediaSentry takes screen shots, which are actual pictures of the screens that MediaSentry or any other user of the peer-to-peer network can see when reviewing the files being distributed. Second, MediaSentry captures as a text file all of the contents of the user's shared directory, such as the names of each file and the size of each file, as well as additional information (called "metadata") about each file. Metadata may include a wide range of information about a file. Metadata, for example, can include information such as identification of the person or group that originally copied the file and began disseminating it unlawfully. MediaSentry does nothing to create this text file; it exists on the user's hard drive and is distributed by the user to anyone to whom the user distributes files.

8. MediaSentry's process for identifying potential infringers and gathering evidence of infringement has multiple fail-safes to ensure that the information gathered is accurate. MediaSentry takes numerous steps to check and double-check the IP address of the potential infringer.

9. MediaSentry followed the procedures outlined above with respect to the evidence that it gathered in this case. Specifically, on August 10, 2004, at approximately 12:49 A.M. EDT, MediaSentry detected the username "sublimeguy14@KaZaA" logged into the KaZaA file-sharing service at IP address 68.227.185.38. Attached as Exhibit B to Plaintiffs' Complaint is a

true and correct copy of a compilation of screen shots captured by MediaSentry on August 10, 2004 showing the list of files that the computer connected to KaZaA with the IP address of 68.227.185.38 was distributing 816 audio files under the username "sublimeguy14@KaZaA" to others for download.

10. Exhibit B indicates that the KaZaA user was "not sharing any files." This indicated that MediaSentry's investigator was not sharing any files.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this 2nd day of January, 2008.

Elizabeth Hardwick

Elizabeth Hardwick

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

ATLANTIC RECORDING CORPORATION, a Delawar corporation; CAPITOL RECORDS, INC., a Delaware corporation; VIRGIN RECORDS AMERICA, INC., a California corporation; INTERSCOPE RECORDS, a California general partnership; UMG RECORDINGS, INC., a Delaware corporation; BMG MUSIC, a New Yor general partnership; SONY BMG MUSIC ENTERTAINMENT, a Delaware general partnership; an ARISTA RECORDS LLC, a Delaware limited liability company,

Plaintiffs,

Case No.: 6:07-cv-06139-DGL

v.

JEFF DANGLER,

Defendant.

DECLARATION OF ELIZABETH HARDWICK

I, Elizabeth Hardwick, pursuant to 28 U.S.C. § 1746, declare as follows:

1. I am the Product Manager, Data Services for the MediaSentry Business Unit of Safenet, Inc., formerly MediaSentry, Inc. ("MediaSentry"). I have personal knowledge of all of the matters discussed in this Declaration except as where stated on information and belief. As to such facts, I believe them to be true.

2. MediaSentry is one of the principal providers of online anti-piracy services worldwide. It specializes in providing services to detect and prevent unauthorized distribution of music, films, software, and other content on the Internet.

3. MediaSentry has been engaged by the Recording Industry Association of America ("RIAA") on behalf of the Plaintiffs to assist them in locating individuals infringing their copyrights over peer-to-peer networks and gathering evidence of their infringement. To perform

this task, MediaSentry searches peer-to-peer networks for individuals distributing infringing files for download and gathers evidence concerning that infringement.

4. In gathering evidence of infringement, MediaSentry does not do anything that any user of a peer-to-peer network cannot do and does not obtain any information that is not available to anyone who logs onto a peer-to-peer network. Thus, when MediaSentry searches for sound recordings on the peer-to-peer network, views the files that each peer-to-peer user is disseminating to others, obtains the IP address and screen name of each user, and downloads copyrighted works distributed by each user, it is using functionalities that are built into the peer-to-peer protocols that each user has chosen to use to upload (or distribute) and download (or copy) music.

5. MediaSentry searches peer-to-peer networks, looking for users distributing ("uploading") files that appear to be digital copies of sound recordings whose copyrights are owned by the RIAA's member record companies. When MediaSentry finds such a file, it may download the file. As part of that downloading process, MediaSentry, like any other peer-to-peer user, receives basic information about the user from whom the work is being downloaded. That information includes, among other things, the Internet Protocol ("IP") address of the user.

6. Once connected to the user's computer, MediaSentry also seeks to determine what other files the individual is distributing to others for download. KaZaA and other file-copying programs permit users to share all of the files in their shared folders, and they may contain a feature that permits users to browse the entire shared folder of another user. When available, MediaSentry invokes this feature of a peer-to-peer program, just as any other user could do, and is able to determine whether the individual user is merely distributing one or two music files or whether the user is distributing hundreds or even thousands of music files.

7. Again using a feature of the peer-to-peer software available to any user, MediaSentry can then capture a list of all of the files that the user is distributing to others for download. MediaSentry collects this information in two forms. First, MediaSentry takes screen shots, which are actual pictures of the screens that MediaSentry or any other user of the peer-to-peer network can see when reviewing the files being distributed. Second, MediaSentry captures as a text file all of the contents of the user's shared directory, such as the names of each file and the size of each file, as well as additional information (called "metadata") about each file. Metadata may include a wide range of information about a file. Metadata, for example, can include information such as identification of the person or group that originally copied the file and began disseminating it unlawfully. MediaSentry does nothing to create this text file; it exists on the user's hard drive and is distributed by the user to anyone to whom the user distributes files.

8. MediaSentry's process for identifying potential infringers and gathering evidence of infringement has multiple fail-safes to ensure that the information gathered is accurate. MediaSentry takes numerous steps to check and double-check the IP address of the potential infringer to prevent misidentification.

9. MediaSentry followed the procedures outlined above with respect to the evidence that it gathered in this case. Specifically, on August 24, 2005, at approximately 6:26 p.m., MediaSentry detected the username "heavyjeffmc@KaZaA" logged into the KaZaA file-sharing service at IP address 172.139.93.233. Attached as Exhibit B to Plaintiffs' Complaint is a true and correct copy of a compilation of screen shots captured by MediaSentry on August 24, 2005 showing the list of files, including digital music files, that the computer connected to KaZaA with the IP address of 172.139.93.233 was distributing, for free, under the username "heavyjeffmc@KaZaA" to others for download. MediaSentry also downloaded a sampling of

the sound recordings that this individual was distributing to other users. A list of eight such sound recordings downloaded by MediaSentry from the KaZaA user heavyjeffmc@KaZaA connected to the Internet at IP address 172.139.93.233 on August 24, 2005, at approximately 6:26 p.m. is attached as Exhibit A to Plaintiffs' Complaint.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this 2nd day of November, 2007.

Elizabeth Hardwick

Elizabeth Hardwick

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION

SONY BMG MUSIC ENTERTAINMENT, *et al.*,	§ § §	
Plaintiffs,	§ §	
vs.	§	CIVIL ACTION NO. 4:06-cv-564-Y
VONDA BLUME,	§ § §	
Defendant.	§ §	

DECLARATION OF ELIZABETH HARDWICK

I, Elizabeth Hardwick, pursuant to 28 U.S.C. § 1746, declare as follows:

1. I am the Product Manager, Data Services for the MediaSentry Business Unit of Safenet, Inc., formerly MediaSentry, Inc. ("MediaSentry"). I have personal knowledge of all of the matters discussed in this Declaration except as where stated on information and belief. As to such facts, I believe them to be true.

2. MediaSentry is one of the principal providers of online anti-piracy services worldwide. It specializes in providing services to detect and prevent unauthorized distribution of music, films, software, and other content on the Internet.

3. MediaSentry has been engaged by the Recording Industry Association of America ("RIAA") on behalf of the Plaintiffs to assist them in locating individuals infringing their copyrights over peer-to-peer networks and gathering evidence of their infringement. To perform this task, MediaSentry searches peer-to-peer networks for individuals distributing infringing files for download and gathers evidence concerning that infringement.

4. In gathering evidence of infringement, MediaSentry does not do anything that any user of a peer-to-peer network cannot do and does not obtain any information that is not

available to anyone who logs onto a peer-to-peer network. Thus, when MediaSentry searches for sound recordings on the peer-to-peer network, views the files that each peer-to-peer user is disseminating to others, obtains the IP address and screen name of each user, and downloads copyrighted works distributed by each user, it is using functionalities that are built into the peer-to-peer protocols that each user has chosen to use to upload (or distribute) and download (or copy) music.

5. MediaSentry searches peer-to-peer networks, looking for users distributing ("uploading") files that appear to be digital copies of sound recordings whose copyrights are owned by the RIAA's member record companies. When MediaSentry finds such a file, it may download the file. As part of that downloading process, MediaSentry, like any other peer-to-peer user, receives basic information about the user from whom the work is being downloaded. That information includes, among other things, the Internet Protocol ("IP") address of the user.

6. Once connected to the user's computer MediaSentry also seeks to determine what other files the individual is distributing to others for download. KaZaA and other file-copying programs permit users to share all of the files in their shared folders, and they may contain a feature that permits users to browse the entire shared folder of another user. When available, MediaSentry invokes this feature of a peer-to-peer program, just as any other user could do, and is able to determine whether the individual user is merely distributing one or two music files or whether the user is distributing hundreds or even thousands of music files.

7. Again using a feature of the peer-to-peer software available to any user, MediaSentry can then capture a list of all of the files that the user is distributing to others for download. MediaSentry collects this information in two forms. First, MediaSentry takes screen shots, which are actual pictures of the screens that MediaSentry or any other user of the peer-to-peer network can see when reviewing the files being distributed. Second, MediaSentry captures

as a text file all of the contents of the user's shared directory, such as the names of each file and the size of each file, as well as additional information (called "metadata") about each file. Metadata may include a wide range of information about a file. Metadata, for example, can include information such as identification of the person or group that originally copied the file and began disseminating it unlawfully. MediaSentry does nothing to create this text file; it exists on the user's hard drive.

8. MediaSentry's process for identifying potential infringers and gathering evidence of infringement has multiple fail-safes to ensure that the information gathered is accurate. MediaSentry takes numerous steps to check and double-check the IP address of the potential infringer to prevent misidentification.

9. MediaSentry followed the procedures outlined above with respect to the evidence that it gathered in this case. Specifically, on May 17, 2004, at approximately 3:21 A.M. EDT, MediaSentry detected the username "blume3611@KaZaA" logged into the KaZaA file-sharing network at IP address 209.30.43.77. Attached as Exhibit B to Plaintiffs' Complaint (Doc. Nos. 2-8) is a true and correct copy of a compilation of screen shots captured by MediaSentry on May 17, 2004 showing the list of files that the computer connected to KaZaA with the IP address of 209.30.43.77 was distributing 1469 music files under the username "blume3611@KaZaA" to others for download.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this _19_th day of July 2007.

Elizabeth Hardwick

Elizabeth Hardwick

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

BMG MUSIC, *et al.*,	§	
	§	
Plaintiffs,	§	
	§	
vs.	§	CIVIL ACTION NO. 1:07-cv-00097-SS-RP
	§	
TEAL SHALEK,	§	
	§	
Defendant.	§	

DECLARATION OF ELIZABETH HARDWICK

I, Elizabeth Hardwick, pursuant to 28 U.S.C. § 1746, declare as follows:

1. I am the Product Manager, Data Services for the MediaSentry Business Unit of Safenet, Inc., formerly MediaSentry, Inc. ("MediaSentry"). I have personal knowledge of all of the matters discussed in this Declaration except as where stated on information and belief. As to such facts, I believe them to be true.

2. MediaSentry is one of the principal providers of online anti-piracy services worldwide. It specializes in providing services to detect and prevent unauthorized distribution of music, films, software, and other content on the Internet.

3. MediaSentry has been engaged by the Recording Industry Association of America ("RIAA") on behalf of the Plaintiffs to assist them in locating individuals infringing their copyrights over peer-to-peer networks and gathering evidence of their infringement. To perform this task, MediaSentry searches peer-to-peer networks for individuals distributing infringing files for download and gathers evidence concerning that infringement.

4. In gathering evidence of infringement, MediaSentry does not do anything that any user of a peer-to-peer network cannot do and does not obtain any information that is not available to anyone who logs onto a peer-to-peer network. Thus, when MediaSentry searches for

sound recordings on the peer-to-peer network, views the files that each peer-to-peer user is disseminating to others, obtains the IP address and screen name of each user, and downloads copyrighted works distributed by each user, it is using functionalities that are built into the peer-to-peer protocols that each user has chosen to use to upload (or distribute) and download (or copy) music.

5. MediaSentry searches peer-to-peer networks, looking for users distributing ("uploading") files that appear to be digital copies of sound recordings whose copyrights are owned by the RIAA's member record companies. When MediaSentry finds such a file, it may download the file. As part of that downloading process, MediaSentry, like any other peer-to-peer user, receives basic information about the user from whom the work is being downloaded. That information includes, among other things, the Internet Protocol ("IP") address of the user.

6. Once connected to the user's computer MediaSentry also seeks to determine what other files the individual is distributing to others for download. KaZaA and other file-copying programs permit users to share all of the files in their shared folders, and they may contain a feature that permits users to browse the entire shared folder of another user. When available, MediaSentry invokes this feature of a peer-to-peer program, just as any other user could do, and is able to determine whether the individual user is merely distributing one or two music files or whether the user is distributing hundreds or even thousands of music files.

7. Again using a feature of the peer-to-peer software available to any user, MediaSentry can then capture a list of all of the files that the user is distributing to others for download. MediaSentry collects this information in two forms. First, MediaSentry takes screen shots, which are actual pictures of the screens that MediaSentry or any other user of the peer-to-peer network can see when reviewing the files being distributed. Second, MediaSentry captures as a text file all of the contents of the user's shared directory, such as the names of each file and

the size of each file, as well as additional information (called "metadata") about each file. Metadata may include a wide range of information about a file. Metadata, for example, can include information such as identification of the person or group that originally copied the file and began disseminating it unlawfully. MediaSentry does nothing to create this text file; it exists on the user's hard drive and is distributed by the user to anyone to whom the user distributes files.

8. MediaSentry's process for identifying potential infringers and gathering evidence of infringement has multiple fail-safes to ensure that the information gathered is accurate. MediaSentry takes numerous steps to check and double-check the IP address of the potential infringer to prevent misidentification.

9. MediaSentry followed the procedures outlined above with respect to the evidence that it gathered in this case. Specifically, on June 10, 2004, at approximately 3:40 A.M. EDT, MediaSentry detected the username "leighpers@KaZaA" logged into the KaZaA file-sharing service at IP address 24.175.59.240. Attached as Exhibit B to Plaintiffs' Complaint is a true and correct copy of a compilation of screen shots captured by MediaSentry on June 10, 2004 showing the list of files that the computer connected to KaZaA with the IP address of 24.175.59.240 was distributing 680 audio files under the username "leighpers@KaZaA" to others for download.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this 29th day of October 2007.

Elizabeth Hardwick
Elizabeth Hardwick

Jonathan G. Fetterly (State Bar No. 228612)
HOLME ROBERTS & OWEN LLP
777 South Figueroa Street, Suite 2800
Los Angeles, CA 90017-5826
Telephone: (213) 572-4300
Facsimile: (213) 572-4400
E-mail: jon.fetterly@hro.com

Attorney for Plaintiffs
VIRGIN RECORDS AMERICA, INC.; SONY BMG MUSIC ENTERTAINMENT; ARISTA RECORDS LLC; and MOTOWN RECORD COMPANY, L.P.

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

VIRGIN RECORDS AMERICA, INC., a California corporation; SONY BMG MUSIC ENTERTAINMENT, a Delaware general partnership; ARISTA RECORDS LLC, a Delaware limited liability company; and MOTOWN RECORD COMPANY, L.P., a California limited partnership, Plaintiffs, v. WENDY CANTOS, Defendant.	Case No.: 06-CV-0915 L (CAB) Hon. James Lorenz **DECLARATION OF ELIZABETH HARDWICK**

DECLARATION OF ELIZABETH HARDWICK

I, Elizabeth Hardwick, pursuant to 28 U.S.C. § 1746, declare as follows:

1. I am the Product Manager, Data Services for the MediaSentry Business Unit of Safenet, Inc., formerly MediaSentry, Inc. ("MediaSentry"). I have personal knowledge of all of the matters discussed in this Declaration except as where stated on information and belief. As to such facts, I believe them to be true.

2. MediaSentry is one of the principal providers of online anti-piracy services worldwide. It specializes in providing services to detect and prevent unauthorized distribution of music, films, software, and other content on the Internet.

3. MediaSentry has been engaged by the Recording Industry Association of America ("RIAA") on behalf of the Plaintiffs to assist them in locating individuals infringing their copyrights over peer-to-peer networks and gathering evidence of their infringement. To perform this task, MediaSentry searches peer-to-peer networks for individuals distributing infringing files for download and gathers evidence concerning that infringement.

4. In gathering evidence of infringement, MediaSentry does not do anything that any user of a peer-to-peer network cannot do and does not obtain any information that is not available to anyone who logs onto a peer-to-peer network. Thus, when MediaSentry searches for sound recordings on the peer-to-peer network, views the files that each peer-to-peer user is disseminating to others, obtains the IP address and screen name of each user, and downloads copyrighted works distributed by each user, it is using functionalities that are built into the peer-to-peer protocols that each user has chosen to use to upload (or distribute) and download (or copy) music.

5. MediaSentry searches peer-to-peer networks, looking for users distributing ("uploading") files that appear to be digital copies of sound recordings whose copyrights are owned by the RIAA's member record companies. When MediaSentry finds such a file, it may download the file. As part of that downloading process, MediaSentry, like any other peer-to-peer user, receives basic information about the user from whom the work is being downloaded. That information includes, among other things, the Internet Protocol ("IP") address of the user.

6. Once connected to the user's computer MediaSentry also seeks to determine what other files the individual is distributing to others for download. KaZaA and other file-copying programs permit users to share all of the files in their shared folders, and they may contain a feature that permits users to browse the entire shared folder of another user. When available, MediaSentry invokes this feature of a peer-to-peer program, just as any other user could do, and is able to determine whether the individual user is merely distributing one or two music files or whether the user is distributing hundreds or even thousands of music files.

7. Again using a feature of the peer-to-peer software available to any user, MediaSentry can then capture a list of all of the files that the user is distributing to others for download. MediaSentry collects this information in two forms. First, MediaSentry takes screen shots, which are actual pictures of the screens that MediaSentry or any other user of the peer-to-peer network can see when reviewing the files being distributed. Second, MediaSentry captures as a text file all of the contents of the user's shared directory, such as the names of each file and the size of each file, as well as additional information (called "metadata") about each file. Metadata may include a wide range of information about a file. Metadata, for example, can include information such as identification of the person or group that originally copied the file and began disseminating it unlawfully. MediaSentry does nothing to create this text file; it exists on the user's hard drive and is distributed by the user to anyone to whom the user distributes files.

8. MediaSentry's process for identifying potential infringers and gathering evidence of infringement has multiple fail-safes to ensure that the information gathered is accurate. MediaSentry takes numerous steps to check and double-check the IP address of the potential infringer to prevent misidentification.

9. MediaSentry followed the procedures outlined above with respect to the evidence that it gathered in this case. Specifically, on October 6, 2004, at approximately 1:31 A.M. EDT, MediaSentry detected the username "tequilaworm@KaZaA" logged into the KaZaA file-sharing service at IP address 68.6.205.97. Attached as Exhibit B to Plaintiffs' Complaint is a true and correct copy of a compilation of screen shots captured by MediaSentry on October 6, 2004 showing

the list of files that the computer connected to KaZaA with the IP address of 68.6.205.97 was distributing 810 audio files under the username "tequilaworm@KaZaA" to others for download.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this 17th day of December 2007.

Elizabeth Hardwick

Elizabeth Hardwick

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

--x

ELEKTRA ENTERTAINMENT GROUP INC., a Delaware :
corporation; VIRGIN RECORDS AMERICA, INC., a
California corporation, UMG RECORDINGS, INC., :
a Delaware corporation; BMG Music, a New York general
partnership; and SONY BMG MUSIC ENTERTAINMENT, :
a Delaware general partnership,

Plaintiffs, : Case No. 05CV2414 (CM)(MDF)

-against- :

PATRICIA SANTANGELO, :

Defendant. :

--x

DECLARATION OF TOM MIZZONE

I, Tom Mizzone, under penalty of perjury, hereby declare and say:

1. I am the Director of the MediaSentry Product Development unit of Safenet, Inc., formerly MediaSentry, Inc. ("MediaSentry"). I have personal knowledge of all of the matters discussed in this Declaration.

2. MediaSentry is one of the principal providers of online anti-piracy services worldwide. It specializes in providing services to detect and prevent unauthorized distribution of music, films, software, and other content on the Internet.

3. MediaSentry has been engaged by the Recording Industry Association of America ("RIAA") on behalf of the Plaintiffs to assist them in locating individuals infringing their copyrights over peer-to-peer networks and gathering evidence of their infringement. In my role at MediaSentry, I have detailed knowledge of the process MediaSentry uses to collect such evidence.

4. In this case, MediaSentry detected the usernames "laxattack857@fileshare" and "mich8621@fileshare" logged into the iMesh file-sharing network from the IP address 24.45.58.150 on numerous separate occasions. In response to those detections, MediaSentry sent instant messages to the computer at the IP address 24.45.58.150 between August 2003 and May 2004. Attached hereto as Exhibit 1 is a true and correct copy of a log of the instant messages which MediaSentry sent to the IP address 24.45.58.150, as well as a true and correct copy of the instant message that was sent.

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

Executed this 12th day of March 2007.

Tom Mizzone