

1. SafeNet objects to the Subpoena on the grounds that the Subpoena will subject it to undue burden in contravention of Rule 45(c)(3)(A)(iii) of the Federal Rules of Civil Procedure, and that Lindor and her attorneys have not taken reasonable steps to avoid imposing undue burden and expense on SafeNet as required under Rule 45(c)(1). The Subpoena calls for the production of voluminous documents concerning its most sensitive proprietary information and contractual or business relationship information, none of which is related to this action. The volume of documents requested by the Subpoena is enormous, and beyond the scope of the underlying action. There is no justification to placing this substantial burden and expense on SafeNet, a non-party in this proceeding.

2. SafeNet objects to the Subpoena pursuant to Rule 45(c)(3)(B)(i) of the Federal Rules of Civil Procedure because it requires disclosure of SafeNet's trade secrets or other confidential research, development, or commercial information. In addition, prior to the disclosure of any privileged, protected, confidential, or proprietary information, SafeNet asserts that the parties must have agreed to a Protective Order entered by the Court. Defendant has refused to attempt to negotiate a mutually-acceptable Protective Order.

3. SafeNet objects to the Subpoena to the extent that it is overly broad, vague and not reasonably calculated to lead to the production of relevant documents.

4. SafeNet objects to the Subpoena to the extent that it calls for the production of documents subject to the attorney-client privilege, work product protection or any other applicable privilege or statutory restriction.

5. SafeNet objects to the Subpoena on the grounds that it seeks documents and information from SafeNet, a non-party, which could be obtained readily from parties to the action.

6. SafeNet objects to the Subpoena to the extent that the Defendant has not agreed to reimburse it for the reasonable costs incurred in producing, assembling and copying the documents sought.

7. SafeNet objects to each Request to the extent that they are duplicative, redundant, vague, ambiguous, unintelligible, intended for the purposes of harassment, call for documents already in the possession of defendants, or call for documents that are plainly available from public sources or as equally available to defendants as SafeNet.

8. SafeNet objects to the definition of "Digital Data" as vague and ambiguous.

9. SafeNet does not waive any of its objections by providing a specific response or by raising additional objections to any specific request for production. It incorporates each of these general objections in each and every one of its responses set forth below.

10. SafeNet's investigation and search for documents responsive to the Requests is ongoing. It will produce additional documents, if any, as they are located. Pursuant to FRCP 26(e), SafeNet reserves the right to supplement its responses and objections, if necessary, to reflect additional information.

11. SafeNet reserves the right to redact material that is irrelevant and non-responsive from any document otherwise to be produced.

12. SafeNet is prepared to discuss any of the objections herein or to attempt to narrow the Requests so that they would not be objectionable.

## **Documents to produce**

**All documents relating to The Account, including but not limited to:**

**1. All documents relating to (a) any investigative licenses, or other licenses having any bearing on The Account, held by MediaSentry, Tom Mizzone ("Mizzone"), and/or any person supervising Mizzone, and (b) the dates, times and locations of any services performed by Mizzone or any other person employed or otherwise associated with MediaSentry having any relationship to The Account.**

In addition to its General Objections, SafeNet objects to this Request on the grounds that it is vague and ambiguous, and calls for the production of documents neither relevant nor reasonably calculated to lead to the discovery of admissible evidence. Without waiving and subject to the general and specific objections, SafeNet refers defendant to the documents attached as exhibits to her Subpoena, as per agreement with her counsel.

**2. (a) All documents sufficient to show all compensation received by MediaSentry from January 1, 2003, to date from the RIAA affiliated companies for any purpose, (b) all documents relating to the specific method, rates, and amounts of compensation applicable to The Account, and (c) all documents relating to the scope of MediaSentry's retention in connection with The Account, including any instructions, guidelines, goals, or parameters.**

In addition to its General Objections, SafeNet objects to this Request on the grounds that it is overly broad, unduly burdensome, vague and ambiguous, calls for the production of documents neither relevant nor reasonably calculated to lead to the discovery of admissible evidence, calls for the production of documents which contain SafeNet and RIAA and its member companies' proprietary and/or confidential information, and calls for the production of documents protected by the attorney-client privilege, work product doctrine or any other applicable protection or privilege. Additionally, SafeNet objects to these requests as the Court has already found them improper when previously directed to the Plaintiffs in this action.

**3. All documents relating to communications of MediaSentry or Mizzone with plaintiffs, plaintiffs' counsel, Matthew J. Oppenheim ("Oppenheim"), the RIAA, and/or Dr. Doug Jacobson, in connection with The Account.**

In addition to its General Objections, SafeNet objects to this Request on the grounds that it calls for the production of documents protected by the attorney-client privilege, work product doctrine or any other applicable protection or privilege. Without waiving and subject to the general and specific objections, SafeNet will produce all non-privileged documents responsive to this request.

**4. Transcripts of any testimony given, and copies of any declarations or affidavits made, by Mizzone or any other MediaSentry representative in any p2p file sharing case in the United States.**

In addition to its General Objections, SafeNet objects to this Request on the grounds that it is overly broad, unduly burdensome, vague and ambiguous, is equally available to defendant as SafeNet calls for the production of documents neither relevant nor reasonably calculated to lead to the discovery of admissible evidence, calls for the production of documents which contain SafeNet proprietary and/or confidential information and/or is covered by a Confidentiality or Protective Order in another litigation.

**5. All reports, memoranda, correspondence, notes and e-mails sent to, or received from plaintiffs, their attorneys and/or the RIAA relating to or concerning The Account.**

In addition to its General Objections, SafeNet objects to this Request on the grounds that it is overly broad, unduly burdensome, and calls for the production of documents protected by the attorney-client privilege and the work product doctrine. Without waiving and subject to the general and specific objections, SafeNet refers defendant to the documents attached as exhibits to her Subpoena, as per agreement with her counsel.

**6. All documents containing, evidencing or otherwise concerning (a) methods and procedures to be used and protocols to be followed for investigating, detecting and monitoring the activity alleged in the complaint, including, but not limited to validation methodology, testing procedures, failure rates and work flow methods, (b) procedures, if any, followed by MediaSentry, during its investigation of the activity alleged in the complaint, for mitigating the misidentification of IP addresses caused by IP address spoofing, (c) procedures followed by MediaSentry, during its investigation of the activity alleged in the complaint, for mitigating the effect and consequences of virus and malware infections, and/or (d) procedures followed by MediaSentry, during its investigation of the activity alleged in the complaint, for ensuring the validity and integrity of information returned by superpeers.**

In addition to its General Objections, SafeNet objects to this Request on the grounds that it calls for the production of documents which contain SafeNet proprietary and/or confidential information. Additionally, SafeNet objects to these requests as the Court has already found (b) and (c) improper when previously directed to the Plaintiffs in this action.

**7. All documents evidencing, reflecting, explaining, referring to or otherwise concerning the setting, synchronization, and maintenance of clock time on the computers and servers that MediaSentry used in the investigation and detection of the activity alleged in the complaint.**

Without waiving and subject to the general and specific objections, SafeNet will produce non-privileged documents responsive to this request.

**8. All documents evidencing, reflecting, or otherwise concerning the amount of time that MediaSentry and its employees and agents were engaged in investigating, detecting and reporting the activity alleged in the complaint.**

In addition to its General Objections, SafeNet objects to this Request on the grounds that it calls for the production of documents which contain SafeNet proprietary and/or confidential information. Without waiving and subject to the general and specific objections, SafeNet will produce non-privileged documents responsive to this request

**9. Complete digital copies of all packet logs of traffic sent to and from the measurement infrastructure and the P2P network in connection with the investigation and detection of the activity alleged in the complaint, including all packet logs of traffic sent to and from the Kazaa bootstrap superpeer and Kazaa session superpeer.**

In addition to its General Objections, SafeNet objects to this Request on the grounds that it is vague and ambiguous, specifically that "measurement infrastructure", "bootstrap superpeer", and "session superpeer" are not defined by defendant. Without waiving and subject to the general and specific objections, SafeNet refers defendant to the documents attached as exhibits to her Subpoena, as per agreement with her counsel.

**10. All documents sufficient to identify the software(s), hardware systems and other tools and devices that were used to detect and monitor the activity alleged in the complaint.**

In addition to its General Objections, SafeNet objects to this Request on the grounds that it is vague and ambiguous, calls for the production of documents neither relevant nor reasonably calculated to lead to the discovery of admissible evidence, and calls for the production of documents which contain SafeNet proprietary and/or confidential information.

**11. Digital copy of the source code of the software(s) used to detect and monitor the activity alleged in the complaint.**

In addition to its General Objections, SafeNet objects to this Request on the grounds that it is overly broad, unduly burdensome, calls for the production of documents neither relevant nor reasonably calculated to lead to the discovery of admissible evidence, calls for the production of documents which contain SafeNet proprietary and/or confidential information, and calls for the production of documents protected by the attorney-client privilege, work product doctrine or any other applicable protection or privilege.

**12. Manuals for the software(s) used to detect and monitor the activity alleged in the complaint.**

In addition to its General Objections, SafeNet objects to this Request on the grounds that it is overly broad, unduly burdensome, vague and ambiguous, calls for the production of documents neither relevant nor reasonably calculated to lead to the discovery of admissible evidence, calls for the production of documents which contain SafeNet proprietary and/or confidential information, and calls for the production of documents protected by the attorney-client privilege, work product doctrine or any other applicable protection or privilege.

**13. Digital copies of all electronic files, including metadata, downloaded or accessed by MediaSentry relating to The Account.**

See Response to request number 1(b).

**14. Digital copies of the Kazaa or other peer to peer software program installed on the computers or servers that MediaSentry used in connection with its investigating, detecting and monitoring the activity alleged in the complaint.**

In addition to its General Objections, SafeNet objects to this Request on the grounds that it is overly broad, unduly burdensome, vague and ambiguous, calls for the production of documents neither relevant nor reasonably calculated to lead to the discovery of admissible evidence, calls for the production of documents which contain SafeNet proprietary and/or confidential information, and calls for the production of documents protected by the attorney-client privilege, work product doctrine or any other applicable protection or privilege.

**15. (A) All documents identifying, evidencing, reflecting or otherwise concerning the software that was used to generate the data in Exhibit A. (B) All documents identifying, evidencing or otherwise concerning (i) the natural person or persons, if any, who generated, or caused to be generated, Exhibit A hereto, and/or (ii) the hardware used to generate, or cause to be generated, said exhibit. (C) Digital copy of the .txt file from which Exhibit A was printed. (D) Digital copies of all files whose data was used in the creation of, or incorporated into, said .txt file.**

In addition to its General Objections, SafeNet objects to this Request on the grounds that it is overly broad, unduly burdensome, vague and ambiguous, calls for the production of documents neither relevant nor reasonably calculated to lead to the discovery of admissible evidence, calls for the production of documents which contain SafeNet proprietary and/or confidential information, and calls for the production of documents protected by the attorney-client privilege, work product doctrine or any other applicable protection or privilege. Without waiving and subject to the general and specific objections, SafeNet will produce non-privileged documents that are responsive to subpart (C) of this request by reference to the documents attached as exhibits to her Subpoena, as per agreement with her counsel.

16. (A) All documents identifying, evidencing, reflecting or otherwise concerning the software that was used to generate the data in Exhibit B. (B) All documents identifying, evidencing or otherwise concerning (i) the natural person or persons, if any, who generated, or caused to be generated, the document annexed hereto as Exhibit B, and/or (ii) the hardware used to generate, or cause to be generated, said exhibit. (C) Digital copy of the .txt file from which Exhibit B was printed. (D) Digital copies of all files whose data was used in the creation of, or incorporated into, said .txt file. (E) A printout of the .txt file from which Exhibit B was printed, which sets forth all of the data in said file, including text that was cut off on the right margin of Exhibit B. (F) All documents identifying, evidencing, reflecting or otherwise concerning (i) "Rule Name: Hubcap" as referred to on the second line of page 1 of Exhibit B, (ii) "agent ID 194" as referred to on the fourth line of page 1 of Exhibit B, and/or (iii) "Scanner Name: DAYSC17" as referred to on the fourth line of page 1 of Exhibit B. (G) Digital copies of the eleven (11) files allegedly downloaded on 8/7/2004 from 6:41:26 AM to 7:08:33 AM, as set forth in Exhibit B. (H) Digital copies of the eleven (11) files for which downloads were logged on 8/7/2004 from 7:09:40 AM to 7:09:43 AM, as set forth in Exhibit B.

In addition to its General Objections, SafeNet objects to this Request on the grounds that it is overly broad, unduly burdensome, vague and ambiguous, calls for the production of documents neither relevant nor reasonably calculated to lead to the discovery of admissible evidence, calls for the production of documents which contain SafeNet proprietary and/or confidential information, and calls for the production of documents protected by the attorney-client privilege, work product doctrine or any other applicable protection or privilege. Without waiving and subject to the general and specific objections, SafeNet will produce non-privileged documents that are responsive to subparts (C), (E), (G) and (H) of this request by reference to the documents attached as exhibits to her Subpoena, as per agreement with her counsel.

17. All documents identifying, evidencing, reflecting or otherwise concerning (A) the software that was used to generate the data in Exhibit C, (B) the algorithm and procedures used to generate the data in Exhibit C, (C) the natural person or persons who generated, or caused to be generated, Exhibit C and the digital version of same.

See the responses to requests numbered 11 and 15.

18. (A) Digital copy of the .txt file from which Exhibit C was printed. (B) Digital copies of all files whose data was used in the creation of, or incorporated into, said .txt file. (C) All documents defining or containing the definition of the term "Distinct Matches" as used in Exhibit C. (D) All documents reflecting, evidencing or otherwise concerning how the .txt file in Exhibit C came to be named "Lindor Marie-UserLog-6190165.txt". (E) All documents identifying, evidencing or otherwise concerning the person or persons who named the .txt file, from which the document annexed hereto as Exhibit C was printed,



**“Lindor Marie-UserLog-6190165.txt”. (F) All documents reflecting, evidencing or otherwise concerning how the IP address 141.155.57.198 came to be included in the .txt file from which Exhibit C was printed.**

In addition to its General Objections, SafeNet objects to this Request on the grounds that it is overly broad, unduly burdensome, vague and ambiguous, calls for the production of documents neither relevant nor reasonably calculated to lead to the discovery of admissible evidence, and calls for the production of documents which contain SafeNet proprietary and/or confidential information. Without waiving and subject to the general and specific objections, SafeNet will produce non-privileged documents that are responsive to subparts (A), (C), and (D) by reference to the documents attached as exhibits to her Subpoena, as per agreement with her counsel.

**19. Digital copies of the file(s) from which the document annexed hereto as Exhibit D was printed.**

In addition to its General Objections, SafeNet objects to this Request on the grounds that it calls for the production of documents which contain SafeNet proprietary and/or confidential information.

**20. All other screenshots, user activity logs, and reports ever generated by MediaSentry in connection with The Account.**

Without waiving and subject to the general and specific objections, SafeNet will produce non-privileged documents that are responsive to this request by reference to the documents attached as exhibits to her Subpoena, as per agreement with her counsel.

**21. All documents identifying, evidencing, reflecting or otherwise concerning (A) the software that was used to generate the data in Exhibit E, (B) the algorithm and procedures used to generate the data in Exhibit E, and (C) the natural person or persons who generated exhibit E, or caused it to be generated.**

See response to request number 17.

**22. (A) Digital copy of the .txt file from which Exhibit E was printed. (B) Digital copies of all files whose data was used in the creation of, or incorporated into, said .txt file. (C) All documents defining or containing the definition of the term “Distinct Matches” as used in Exhibit E. (D) All documents reflecting, evidencing or otherwise concerning (i) how the .txt file, from which Exhibit E was printed, came to be named “Lindor Marie-UserLog(Compressed)-6190165.txt”, (ii) the natural person or persons who named the .txt file, from which Exhibit E was printed, “Lindor Marie-UserLog(Compressed)-6190165.txt”, (iii) how the IP address 141.155.57.198 came to be included in the .txt file from which Exhibit E was printed. (E) All documents identifying, evidencing, referring to,**

or otherwise concerning the natural person at MediaSentry who on August 7, 2004 at 6:15 a.m. "detected an individual who was engaged in the distribution of Plaintiff's copyrighted sound recordings using the screen name jrlindor@kazaa and Internet Protocol ("IP") address 141.155.57.198," as alleged on page 5 of Exhibit F. In the event no such documents are produced indicate whether it is because the documents are unavailable, or whether it is because there was no 'detection of an individual'

In addition to its General Objections, SafeNet objects to this Request on the grounds that it is overly broad, unduly burdensome, vague and ambiguous, calls for the production of documents neither relevant nor reasonably calculated to lead to the discovery of admissible evidence, and calls for the production of documents which contain SafeNet proprietary and/or confidential information. Without waiving and subject to the general and specific objections, SafeNet will produce non-privileged documents that are responsive to subparts (A), (C), and (D)(i) by reference to the documents attached as exhibits to her Subpoena, as per agreement with her counsel.

**23. Curriculum vitae and other documents representing, evidencing or otherwise concerning the technical background and experience of the natural person(s) referred to above, and any other persons who will or may testify at the trial of this action, who are employees or agents of MediaSentry.**

In addition to its General Objections, SafeNet objects to this Request on the grounds that it is vague and ambiguous and calls for the production of documents which contain SafeNet proprietary and/or confidential information.

**24. All documents identifying, evidencing, referring to, or otherwise concerning the natural person or persons, if any, at MediaSentry who listened to downloaded files with respect to The Account for the purpose of determining the nature and content of such files.**

There are no such documents.

**25. All documents identifying, evidencing, referring to, or otherwise concerning the date, time and location that downloaded files with respect to The Account were listened to.**

SafeNet objects to this Request on the grounds that it is unintelligible as written.

**26. All memoranda, notes, emails, reports, correspondence and other documents written, created or prepared by the natural person(s) referred to above concerning The Account.**

In addition to its General Objections, SafeNet objects to this Request on the grounds that it calls for the production of documents protected by the attorney-client privilege, work product doctrine or any other applicable protection or privilege. Without waiving and subject to the

general and specific objections, SafeNet will produce non-privileged documents responsive to this request by reference to the documents attached as exhibits to her Subpoena, as per agreement with her counsel.

**27. All documents relating to any attempts by MediaSentry, or any other person or entity, to verify the accuracy of Verizon's subpoena response, and all documents relating to the accuracy and/or synchronization of server clocks and logging instruments at Verizon, and the actual DHCP logs for that day.**

There are no such documents in SafeNet's possession.

**28. All documents relating to any attempts by MediaSentry, or any other person or entity, to verify that any person was using an "online media distribution system" through defendant's internet access account after August 7, 2004.**

There are no such documents in SafeNet's possession.

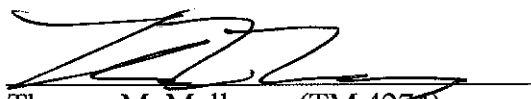
**29. All contracts and agreements between MediaSentry and the Recording Industry Association of America, Inc. ("RIAA") or between MediaSentry and any of the RIAA's affiliated companies, including plaintiffs, relating to The Account.**

Defendant has withdrawn this request

Dated: New York, New York  
January 25, 2008

LAW OFFICES OF THOMAS M. MULLANEY

By:



Thomas M. Mullaney (TM 4274)

708 Third Avenue, Suite 2500  
New York, NY 10017  
Attorneys for SafeNet, Inc.  
(212) 223-0800  
(212) 661-9860 (facsimile)

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

-----X  
UMG RECORDINGS, INC., et al.,

05 CV 1095 (DGT)(RML)

Plaintiffs,

- against

MARIE LINDOR,

Defendant  
-----X

**DECLARATION OF TOM MIZZONE IN OPPOSITION TO  
DEFENDANT'S MOTION IN LIMINE**

I, TOM MIZZONE, declare:

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 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. Once MediaSentry has the list of files being distributed, it searches the list of files for copyrighted works owned by the record companies, just as any other user could do. Once MediaSentry has found a user disseminating files that appear to be copyrighted works owned by the record companies, MediaSentry downloads a sampling of these files, again, as any other peer-to-peer user could do.

9. At the end of its evidence gathering with respect to any individual user, MediaSentry has gathered substantial evidence, including (1) a sampling of individual audio files that the individual is making available in his or her shared directory; (2) a user log identifying all of the files that the individual was distributing for download, as well as metadata about each of the files being distributed; (3) screen shots of the user's shared directory that show the files the individual was distributing; and (4) the IP address, date, and time of the infringement, as well as

the alias or username (when available) chosen by the individual when participating in the peer-to-peer network. MediaSentry does nothing to create any of this data. It exists on the user's hard drive. MediaSentry merely collects such data.

10. 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.

11. MediaSentry followed the procedures outlined above with respect to the evidence that it gathered in this case. Specifically, on August 7, 2004 at approximately 6:15 A.M. EDT, MediaSentry detected the username "jrlindor@KaZaA" logged into the KaZaA file-sharing network at IP address 141.155.57.198. Attached as Exhibit A is a true and correct copy of a compilation of screen shots captured by MediaSentry on August 7, 2004 showing the list of files that the computer connected to KaZaA with the IP address of 141.155.57.198 was distributing to others for download.

12. Consistent with the procedures noted above, on August 7, 2004 at approximately 6:15 A.M. EDT, MediaSentry downloaded a sampling of .MP3 "audio" files from the IP address 141.155.57.198. A true and correct listing of the sampling of audio files that MediaSentry downloaded is attached as Exhibit B. This list is a subset of the sound recordings found on the shared folder shown in Exhibit A. Exhibit C is also a subset of the sound recordings found on the shared folder shown in Exhibit A, and it is true and correct.

13. Exhibit D is a true and correct copy of the SystemLog.txt file captured by MediaSentry while connected to the computer that was connected to the Internet through IP

address 141.155.57.198 on August 7, 2004 at approximately 6:15 A.M. EDT. MediaSentry did not create this data. Rather, it was created automatically when MediaSentry's computer communicated with the computer that was connected to the Internet through IP address 141.155.57.198 on August 7, 2004 at approximately 6:15 A.M. EDT.

14. Exhibit E is a true and correct copy of the UserLog (compressed) .txt file captured by MediaSentry while connected to the computer that was connected to the Internet through IP address 141.155.57.198 on August 7, 2004 at approximately 6:15 A.M. EDT.

15. Exhibit F is a true and correct copy of the UserLog.txt file captured by MediaSentry while connected to the computer that was connected to the Internet through IP address 141.155.57.198 on August 7, 2004 at approximately 6:15 A.M. EDT.

16. Exhibit G is a true and correct copy of the DownloadData.txt file captured by MediaSentry while connected to the computer that was connected to the Internet through IP address 141.155.57.198 on August 7, 2004 at approximately 6:15 A.M. EDT.

17. Exhibit H is a true and correct copy of the Traceroute.txt file captured by MediaSentry while connected to the computer that was connected to the Internet through IP address 141.155.57.198 on August 7, 2004 at approximately 6:15 A.M. EDT.

18. MediaSentry did not create the files attached as Exhibits E-H. These files existed on the hard drive of the computer that was connected to the Internet through IP address 141.155.57.198 on August 7, 2004 at approximately 6:15 A.M. Media Sentry merely captured this data.



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

Executed this \_\_\_\_ day of May, 2007 at New York, New York.

\_\_\_\_\_  
TOM MIZZONE

**Thomas Mullaney**

---

**From:** Tom Mizzone

**Sent:** Monday, May 14, 2007 10:07 AM

**To:** Patricia Kelly

**Subject:** qpjx01! (2).DOC

Can you print? I need to sign / scan / and email.

SN 007

1/22/2008

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

-----X  
UMG RECORDINGS, INC., et al.,

05 CV 1095 (DGT)(RML)

Plaintiffs,

- against

MARIE LINDOR,

Defendant  
-----X

**DECLARATION OF TOM MIZZONE IN OPPOSITION TO  
DEFENDANT'S MOTION IN LIMINE**

I, TOM MIZZONE, declare:

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 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.

Deleted: it

8. Once MediaSentry has the list of files being distributed, it searches the list of files for copyrighted works owned by the record companies, just as any other user could do. Once MediaSentry has found a user disseminating files that appear to be copyrighted works owned by the record companies, MediaSentry downloads a sampling of these files, again, as any other peer-to-peer user could do.

9. At the end of its evidence gathering with respect to any individual user, MediaSentry has gathered substantial evidence, including (1) a sampling of individual audio files that the individual is making available in his or her shared directory; (2) a user log identifying all of the files that the individual was distributing for download, as well as metadata about each of the files being distributed; (3) screen shots of the user's shared directory that show the files the individual was distributing; and (4) the IP address, date, and time of the infringement, as well as

the alias or username (when available) chosen by the individual when participating in the peer-to-peer network. MediaSentry does nothing to create any of this data. It exists on the user's hard drive. MediaSentry merely collects such data.

10. 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.

11. MediaSentry followed the procedures outlined above with respect to the evidence that it gathered in this case. Specifically, on August 7, 2004 at approximately 6:12 A.M. EDT, MediaSentry detected the username "jrlindor@KaZaA" logged into the KaZaA file-sharing network at IP address 141.155.57.198. Attached as Exhibit A is a true and correct copy of a compilation of screen shots captured by MediaSentry on August 7, 2004 showing the list of files that the computer connected to KaZaA with the IP address of 141.155.57.198 was distributing to others for download.

Deleted: 15

12. Consistent with the procedures noted above, on August 7, 2004 at approximately 6:15 A.M. EDT, MediaSentry downloaded a sampling of .MP3 "audio" files from the IP address 141.155.57.198. A true and correct listing of the sampling of audio files that MediaSentry downloaded is attached as Exhibit B. This list is a subset of the sound recordings found on the shared folder shown in Exhibit A. Exhibit C is also a subset of the sound recordings found on the shared folder shown in Exhibit A, and it is true and correct.

13. Exhibit D is a true and correct copy of the SystemLog.txt file captured by MediaSentry while connected to the computer that was connected to the Internet through IP

address 141.155.57.198 on August 7, 2004 at approximately 6:12 A.M. EDT. MediaSentry did not create this data. Rather, it was created automatically when MediaSentry's computer communicated with the computer that was connected to the Internet through IP address

Deleted: 15

141.155.57.198 on August 7, 2004 at approximately 6:12 A.M. EDT.

Deleted: 15

14. Exhibit E is a true and correct copy of the UserLog (compressed) .txt file captured by MediaSentry while connected to the computer that was connected to the Internet through IP address 141.155.57.198 on August 7, 2004 at approximately 6:12 A.M. EDT.

Deleted: 15

15. Exhibit F is a true and correct copy of the UserLog.txt file captured by MediaSentry while connected to the computer that was connected to the Internet through IP address 141.155.57.198 on August 7, 2004 at approximately 6:12 A.M. EDT.

Deleted: 15

16. Exhibit G is a true and correct copy of the DownloadData.txt file captured by MediaSentry while connected to the computer that was connected to the Internet through IP address 141.155.57.198 on August 7, 2004 at approximately 6:15 A.M. EDT.

17. Exhibit H is a true and correct copy of the Traceroute.txt file captured by MediaSentry while connected to the computer that was connected to the Internet through IP address 141.155.57.198 on August 7, 2004 at approximately 6:15 A.M. EDT. ←?

18. MediaSentry did not create the files attached as Exhibits E-H. These files existed on the hard drive of the computer that was connected to the Internet through IP address 141.155.57.198 on August 7, 2004 at approximately 6:12 A.M. Media Sentry merely captured this data.

Deleted: 15

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

Executed this \_\_\_\_ day of May, 2007 at New York, New York.

TOM MIZZONE



**Thomas Mullaney**

---

**From:** Elizabeth Hardwick

**Sent:** Friday, May 11, 2007 11:04 AM

**To:** Tom Mizzone

**Subject:** Re: FW: UMG Recordings v. Lindor

CaseID: 6190165

SN 014

1/22/2008

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF PENNSYLVANIA

MOTOWN RECORD COMPANY, L.P., a  
California limited partnership; CAPITOL  
RECORDS, INC., a Delaware corporation;  
ATLANTIC RECORDING  
CORPORATION, a Delaware corporation;  
UMG RECORDINGS, INC., a Delaware  
corporation; WARNER BROS. RECORDS  
INC., a Delaware corporation; and SONY  
MUSIC ENTERTAINMENT INC., a  
Delaware corporation,

Plaintiffs,

v.

THERESA DEPIETRO,

Defendant.

CIVIL ACTION NO. 2:04-CV-02246-ER

JUDGE EDUARDO C. ROBRENO

MAGISTRATE CYNTHIA M. RUFÉ

**AFFIDAVIT OF THOMAS CARPENTER IN SUPPORT OF PLAINTIFFS' MOTION  
FOR SUMMARY JUDGMENT**

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

**BACKGROUND AND EXPERTISE**

1. I am Director, Data Services for the MediaSentry ("MediaSentry") business unit of SafeNet, Inc. I have personal knowledge of all of the matters discussed in this Affidavit.
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 supervise this evidence collection effort and have detailed knowledge of the process MediaSentry uses to collect such evidence.

#### **THE INTERNET AND PEER-TO-PEER FILE COPYING**

4. The Internet is a vast collection of interconnected computers and computer networks that communicate with each other by telecommunication. The Internet allows hundreds of millions of people around the world to communicate easily and to exchange e-mail, ideas, information, and their own creative works. It also, has allowed companies, non-profit institutions, educational establishments, and even governments to provide, to the vast online public, a wide range of information, services, and even copyrighted material that they have developed or licensed.

5. The Internet has also become a forum for mass reproduction and distribution of *unauthorized* copies of copyrighted material, particularly sound recordings. Once a sound recording has been copied from its original medium (such as a compact disc ("CD")) onto a computer (usually in digital "MP3" or "WMA" format), an unlimited number of further copies can be made, and can be transmitted an unlimited number of times over the Internet, without significant degradation in sound quality.

6. Much of the unauthorized copying and dissemination of copyrighted sound recordings over the Internet occurs via "peer-to-peer" ("P2P") file copying. The most notorious example to date was the original Napster service, which closed in 2001 following a United States federal court injunction.

7. Although Napster no longer exists as a peer-to-peer service, several other peer-to-peer file-copying services and networks, including FastTrack (to which several file-copying programs, such as KaZaA, KaZaA Lite, and Grokster, among others, connect), Gnutella, and

eDonkey, continue to operate and to offer users various means of reproducing and transmitting music files over the Internet.

8. Becoming a user of a peer-to-peer network is relatively straightforward. One need only download peer-to-peer software from any one of dozens of websites, including but not limited to those referenced in paragraph 7, and install that software on one's computer. Once the software has been installed, the user is able to (1) copy files (including sound recordings) onto the user's computers and make those files available for copying and distribution to other users over the Internet; (2) search for files being distributed by other users who are connected to the peer-to-peer service; and (3) transmit exact copies of files from one computer to another via the Internet.

9. Peer-to-peer software allows users to choose what files they wish to distribute to others. Individuals place files on their computer that they want other Internet users to view and download in a separate directory, often referred to as a "shared directory." Once the individual logs onto a peer-to-peer network (by choosing to run peer-to-peer software on a computer that is connected to the Internet), he or she makes all of the files in the shared directory available for searching, copying, and downloading.

10. Peer-to-peer users search the share directories of other users connected to the peer-to-peer system to find files that they would like to copy. Thus, peer-to-peer users can search for files with titles that indicate that they are popular sound recordings. Once such a file is found on another computer, the peer-to-peer user (the "downloader") requests a copy of a file that is in the distributor's ("uploader's") share directory. Using the protocol defined by the peer-to-peer application, the request is sent to the uploader's computer, the file is copied, and the file is then sent to the downloader's computer over the Internet. As with other forms of

communication over the internet, the file is first broken up into packets of data by the uploader's computer, sent over the Internet in multiple packets, and then reassembled into the file at the downloader's computer.

11. Accordingly, when a peer-to-peer user copies a music file into a shared directory and connects to the peer-to-peer service, he or she authorizes massive numbers of other peer-to-peer users to search his or her computer for that file, and also authorizes, facilitates and participates in copying and distribution of copies of that sound recording to other users over the Internet.

12. Typically, there are hundreds of thousands or even millions of users logged onto a peer-to-peer service at any one time. Assuming typical transmission speeds of peer-to-peer users' Internet connections and the size of typical sound recording files, any one file distributed on a peer-to-peer service could be copied and further distributed over the Internet hundreds or thousands of times per day.

#### **UNCOVERING INFRINGERS ON PEER-TO-PEER NETWORKS**

13. As noted above, MediaSentry has been engaged by the RIAA on behalf of the Plaintiffs in these cases to assist them in stopping the infringement of their copyrights. To perform this task, MediaSentry searches peer-to-peer networks for individuals distributing infringing files for download and gathers evidence concerning that infringement.

14. 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.

15. 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 IP (Internet Protocol) address of the user. An IP address is a number that, along with the date and time, can be used to identify a computer using the Internet.

16. 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 "share" folders, and they may contain a feature that permits users to browse the entire share folder of another user. When available, MediaSentry invokes this feature of a peer-to-peer program 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.

17. Again using a feature of the peer-to-peer software, MediaSentry may 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 creates a text file that includes all of the information on the screen shots, 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.

18. Once MediaSentry has the list of files being distributed, it searches the list of files for copyrighted works owned by the record companies. As shown in the example discussed later in this declaration, files distributed by peer-to-peer users generally specify the name and artist of the song being disseminated, as well as the file type ("audio" for most music files) so it is relatively simple to identify files that are likely to be copyrighted sound recordings. In most cases involving peer-to-peer users distributing hundreds or thousands of files for download, this search process uncovers substantial numbers of files that appear to be sound recordings whose copyrights are owned by the record companies.

19. Once MediaSentry has found a user disseminating files that appear to be copyrighted works owned by the record companies, MediaSentry may download (as any other peer-to-peer user could) a sampling of files that appear to be infringing. MediaSentry downloads each of these files in full.

20. At the end of its evidence gathering with respect to any individual user, MediaSentry has gathered substantial evidence, including (1) a sampling of individual audio files that the individual is making available in his or her shared directory; (2) a user log identifying all of the files that the individual was distributing for download, as well as metadata about each of the files being distributed; (3) screen shots of the user's share directory that show the files the individual was distributing; and (4) the IP address, date, and time of the infringement, as well as the alias chosen by the individual (the user name) when participating in the peer-to-peer network.



21. 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. MediaSentry also undertakes substantial and frequent audits to make certain that all of its systems are functioning correctly.

22. Once it has collected this evidence, MediaSentry provides it to the RIAA.

**EVIDENCE COLLECTED WITH RESPECT TO THE DEFENDANT IN THIS CASE**

23. MediaSentry followed the procedures outlined about with respect to the evidence it gathered against the Defendant in this case. To be clear, MediaSentry did not actually identify Ms. DePietro, but identified a particular IP address, which was later identified by her internet service provider, as belonging to her.

24. In this instance, between November 5, 2003 and April 12, 2004, MediaSentry detected the username "ELTONJOHN@KaZaA" logged into the KaZaA file-sharing network from the IP address 216.15.109.54 thirty-two (32) separate times. Attached as Exhibit 1 is a spreadsheet listing the exact date and times. In response to those detections, MediaSentry sent instant messages to the computer at the IP address 216.15.109.54. Those messages "pop-up" on the computer connected to the internet and warn the individual that they are infringing on Plaintiffs' copyrights and that they need to stop. Attached as Exhibit 2 are examples of the instant messages MediaSentry sent to the IP address 216.15.109.54. Those instant messages remain on the screen until the computer user actively closes the messages, either by clicking on the "OK" button or the "X" at the top right-hand corner of the message. While MediaSentry cannot conclusively state that the owner of that computer at the IP address 216.15.109.54 received the messages, MediaSentry got no indications that its messages failed. Similar to email messages, instant messages that fail to reach their destination typically result in an error message



being returned to the sender. In this instance, MediaSentry did not receive any messages that indicated any of its thirty-two instant messages sent to the IP address 216.15.109.54 failed.

25. On November 18, 2003, at 07:03:30 a.m. Eastern Standard Time, MediaSentry discovered ELTONJOHN@KaZaA was logged onto the KaZaA file-copying network. The individual was using the IP address 216.15.109.54 at that time.

26. Attached as **Exhibit 3** to this Affidavit is a 'compilation of screen shots showing the list of files that the computer connected to KaZaA with the IP address of 216.15.109.54 was distributing to others for download. The screen shots in **Exhibit 4** reveal a host of information about the owner of that IP address and the files that that individual was distributing. As shown in the first column, under "user," the IP address 216.15.109.54 in this case was operating under the alias "ELTONJOHN@KaZaA" at the time that IP address was discovered distributing files for download. The second and third columns list the file names of the individual files IP address 216.15.109.54 was distributing on November 18, 2003 as well as the name of an "artist" associated with each file. As is obvious from a review of the file names and artists, many of the files appear to be sound recordings by well-known artists, such as Bruce Springsteen, Frank Sinatra, Matchbox Twenty, Ray Charles, and Elton John. The fourth column lists the size of each file; most of the file sizes, between 1,000 KB (kilobytes) and 8,000 KB are consistent with the file size one would expect for a digital copy of a sound recording in mp3 format. Finally, the fifth column indicates the media type of each file; this column indicates that the vast majority of files being disseminated by IP address 216.15.109.54 are audio files.

27. There are a number of pieces of information at the bottom of the screen shots, in what is called the "status bar." First, the status bar shows the number of files that IP address 216.15.109.54 was distributing on the peer-to-peer network. Of the 1353 total files, 1203 are

MP3, or audio files. Second, the status bar indicates an approximate number of users who were logged onto the KaZaA network at the time the evidence was collected and the number of files being shared by those users – 3,086,814 users sharing over 574 million files. While on the network, the owner of IP address 216.15.109.54 would have had access to download from among those files (just as MediaSentry did) and other users would have had access to the files in the computer's shares folder. Third, in the right corner of the status bar is the phrase "not sharing any files." That refers to MediaSentry's computer, which is configured so that it does not offer any files to other users and thus was not sharing any files at the time this evidence was collected. In contrast, IP address 216.15.109.54 was distributing 1203 audio files to any interested user over the KaZaA network at the time Plaintiffs' evidence was collected; indeed, there would be no other way for MediaSentry to have discovered IP address 216.15.109.54 if the computer's owner had not loaded peer-to-peer software onto it and left the file-sharing mechanisms turned on.

28. As with all individuals who are detected engaging in copyright infringement using a peer-to-peer system, on November 18, 2003 at approximately 7:07:31 a.m. EST, MediaSentry downloaded a sampling of MP3 "audio" files from the IP address 216.15.109.54. The titles to those MP3 files are as follows:

- (a) "Diana Ross – I'm Coming Out (1).mp3"
- (b) "Norah Jones – Don't know why.mp3"
- (c) "Genesis – Invisible Touch.mp3"
- (d) "Rod Stewart – Don't Come Around Here.mp3"
- (e) "U2 – where the Streets have No Name.mp3"
- (f) "Leo Sayer – When I need You.mp3"
- (g) "Dixie Chicks – Goodbye Earl.mp3"

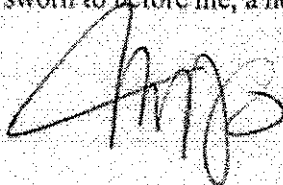
29. Copies of those MP3 files were turned over as evidence to the RIAA.

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

Executed on this 22 day of June, 2006, in Morristown, NJ.

  
Thomas Carpenter

Subscribed and sworn to before me, a notary public, this 22<sup>nd</sup> day of June, 2006.



MARIA DI POPOLO  
NOTARY PUBLIC  
STATE OF NEW JERSEY  
My Commission Expires Apr. 7, 2010