





June 6, 2008

Department of Labor & Economic Growth  
Bureau of Commercial Services – Enforcement Division  
P.O. Box 30018  
Lansing, MI 48909

RE: Media Sentry, Inc.

Dear Sir or Madam:

I am a student at the University of Michigan who has been the subject of intrusive and illegal investigation by a company called Media Sentry, Inc. This company has engaged in an extensive investigation of my activity on university computer servers in an effort to determine 1) my personal identity, 2) my conduct and activities on the internet, and 3) the contents and nature of files within my personal computer. These efforts were undertaken by Media Sentry as part of an investigation into my alleged involvement or responsibility for suspected instances of copyright infringement and to secure, compile and document evidence to be used against me before a court in litigation regarding these alleged activities. Media Sentry advertises itself as a company that specializes in the investigation of intellectual property rights and all of these investigative actions were undertaken by Media Sentry for paid clients within the recording industry. Copies of its company web pages proclaiming and advertising its investigative abilities and services are attached to this complaint.

All of these activities would clearly constitute the activities of a “private investigator” under the Private Detective Licensing Act and as such Media Sentry would be required to have a private investigator license to engage in such activities within the state. All of these investigative actions by Media Sentry, however, were illegal because Media Sentry is not, and has never been, properly licensed as an investigating agency within the State of Michigan. More importantly, all of the investigative actions taken by Media Sentry in its investigation of me and my activities took place after they were warned in writing by your office of their need to immediately secure a license from your office to engage in such activity within the State of Michigan. A copy of your February 22, 2008 warning letter to Media Sentry is attached to this complaint.

This letter is a formal complaint letter to your office regarding the ongoing and continuing activities of this company in investigating the activities and conduct of University students without being licensed as required by Michigan law. Since this company has already been issued a letter from your Department regarding its need to immediately obtain a license to engage in these activities, this letter would request that your office issue a cease and desist letter to this company in light of its ongoing violation of your licensing requirements.

In correspondence to the University of Michigan detailing the investigation results of Media Sentry into my personal activities and conduct, I have been identified simply as

Case #162983070. At this point in time, despite the intrusive investigation of my personal computer files and internet activities by Media Sentry, it is claimed that my personal name and address is unknown to Media Sentry. Accordingly, I am making this complaint to your office under the pseudonym of *Case #162983070*. I am currently represented by Attorney K. Orlando Simon of the University of Michigan's Student Legal Services and all communications and inquiries regarding this complaint can and should be directed to his attention. He will promptly pass along any and all such communications along to me. Attorney K. Orlando Simon's address is Student Legal Services, 2304 Michigan Union, 530 South State Street, #549, Ann Arbor, MI 48109.

On February 22, 2008, Media Sentry was informed by the Commercial Enforcement Division of the Department of Labor & Economic Growth ("DLEG") that its activities might be in violation of Michigan's licensing regulations governing investigative agencies and instructed that "[i]f you intend to perform activities that require a private detective agency license, you must obtain a license immediately." In response to that letter, Media Sentry has not contacted the DLEG to secure a private detective license for its activities. Nor has it sought a determination from the DLEG that its activities in investigating University of Michigan students, and the University's own proxy server, are somehow exempt from applicable licensing regulations. Instead, as documented by the numerous intercepts secured after that date by Media Sentry and the recording industry's latest enforcement request to the University, Media Sentry's response has been to continue its unlicensed and illegal actions within the state by actively investigating University students. Specifically, in my case, Media Sentry has attempted to identify me through an Internet Protocol ("IP") address that was intercepted by them on March 18, 2008, almost a month after your office issued its warning letter. A copy of this interception by Media Sentry documenting the March 2008 intercept is attached to this complaint letter.

That Media Sentry's activities in investigating University of Michigan students would appear to be beyond dispute or question. The Michigan Private Detective License Act ("PDLA") defines "private detective" or "private investigator" in relevant part as a person, who, for a fee, reward or other consideration, engages in business or accepts employment to furnish, or subcontracts or agrees to make, an investigation for the purpose of obtaining information with reference to any of the following:

- ...
- (ii) The identity, habits, conduct, business, occupation, honesty, integrity, credibility, trustworthiness, efficiency, loyalty, activity, movement, whereabouts, affiliations, associations, transactions, acts, reputation, or character of a person,
- ...
- (iv) The cause or responsibility for ... losses, accidents or damage or injury to persons or property,
- (v) Securing evidence to be used before a court ...

For the past year, Media Sentry's investigative activities of university students across Michigan have been repeatedly described and documented under oath by the RIAA in virtually identical affidavits that have been filed in Michigan federal courts. In numerous infringement cases filed against unknown university students, the RIAA has justified its need for extraordinary ex parte discovery orders by reliance upon the results of the investigative efforts of Media Sentry. Carlos Linares, Vice President of the RIAA has filed a supporting declaration in the following Michigan federal court cases detailing the investigative activities of Media Sentry:

Date Filed	Case Name	District	Docket No.
5/3/07	Arista v. Does 1-12	Western	07-00445
5/17/07	London-Sire v. Does 1-18	Eastern	07-12134
5/17/07	Priority v. Does 1-12	Eastern	07-12133
9/20/07	LaFace v. Does 1-5	Western	07-0187
10/7/07	Arista v. Does 1-4	Western	07-0115
11/28/07	Arista v. Does 1-5	Eastern	07-15053
2/21/08	Atlantic v. Does 1-22	Eastern	08-10728
5/28/08	LaFace v. Does 1-21	Eastern	08-12289

I have attached a copy of the most recently filed declaration for your review as part of this complaint. The declaration in all of these cases is nearly identical and details the investigation efforts of Media Sentry in the following terms:

...

11. In order to assist its members in combating copyright piracy, the RIAA retained a third-party investigator, MediaSentry, Inc. ("MediaSentry"), to conduct searches of the Internet, as well as file-copying services, for infringing copies of sound recordings whose copyrights are owned by RIAA members. ... *In gathering evidence of copyright infringement, MediaSentry uses the same functionalities that are built into P2P programs that any user of the software can use on the network.*
12. ...
13. *MediaSentry finds individuals using P2P networks to share music files over the Internet. Just as any other user on the same P2P networks as these individuals would be able to do, MediaSentry is able to detect the infringement of copyrighted works and identify the users' IP addresses because the P2P software being used by those individuals has file-sharing features enabled.*

14. *For each suspected infringer, MediaSentry downloads a number of the music files that the individual is offering to other users on the P2P network. ... MediaSentry assigns an identification number to each individual for which it detects copyright infringement and gathers additional evidence for each individual, such as metadata accompanying each file being disseminated that demonstrates that the user is engaged in copyright infringement. That evidence includes download data files that show for each music file the source IP address, user logs that include a complete listing of all files in the individual's share folder at the time, and additional data that track the movement of the files through the Internet.*
15. *After MediaSentry collects the evidence of infringement, the RIAA engages in a painstaking process to verify whether each individual was infringing. ... The RIAA also reviews the other evidence collected by MediaSentry.*  
(emphasis supplied)

All of the above-noted sworn statements regarding the activities of Media Sentry would clearly establish that its activities fall within the scope of the investigative activities regulated by the PDLA. Nevertheless, Media Sentry has ignored any suggestion by the DLEG that it secure a license to continue its investigative activities within the state of Michigan. In the case of *LaFace v. Does 1-21* (Eastern District 08-1229), involving allegations of copyright infringement by students at Central Michigan University, the recording companies not only attached a copy of the declaration of Carlos Linares but also attached a listing of the intercepted IP address of the alleged infringers. Those intercepted IP addresses documented seven instances of interceptions that took place after the Department's February 22, 2008 letter informing Media Sentry of its need to licensed to conduct such activities. Copies of these intercepted IP addresses are attached to this complaint.

More importantly from my own personal and privacy perspective, Media Sentry continues to flaunt any requirement that it secure an investigation license from your Department with respect to its current and ongoing investigation of students at the University of Michigan. Its investigation of my own alleged conduct in this matter took place almost a month after the issuance of your department's warning letter. In addition, I am aware that I am but one of 15 other University of Michigan students whose personal computer accounts was subject to investigation by Media Sentry in this latest enforcement effort.

Challenges and objections to the failure of Media Sentry to secure appropriate and required state licensure as a private investigative agency have not been limited to the state of Michigan. The unlicensed activity of Media Sentry as a private investigative agency has been challenged in federal court cases in at least eight states including (in chronological order):

Florida	June 1, 2007	UMG v. Suze Del Cid	(07-00368)
Texas	July 2, 2007	BMG v. Rhonda Crain	(06-0567)
Oregon	November 28, 2007	Arista v. Does	(07-06197)

Michigan	March 4, 2008	LaFace v. Does	(07-0187)
Massachusetts	April 9, 2008	London-Sire v. Does	(04-12434)
Maine	April 14, 2008	Atlantic v. Does	(08-28)
North Carolina	April 29, 2008	BMG v. Does	(08-1350)
Arizona	May 6, 2008	Capital v. Weed	(06-01124)

I believe that the investigative tactics and procedures that are employed by Media Sentry are not substantially different from one state to the other and that their activities clearly constitute investigative activities as defined by these various states.

Massachusetts and Maine, which have definitional statutes similar to Michigan's, have each issued cease and desist letters to Media Sentry regarding its investigative activities. I have attached copies of these letters to this complaint. In neither of these states has Media Sentry subsequently applied to be licensed as directed by these letters. Nor, in either state, has it sought a determination from the licensing board that its activities were exempt from licensing requirements. In stark contrast to its apparent compliance with these cease and desist letters, however, Media Sentry apparently has chosen to willfully ignore the recommendations of the DLEG's February 22, 2008 letter and is continuing its activities in an unlicensed and illegal manner against myself and other University of Michigan students.

It is apparent that Media Sentry feels no obligation to secure a license from the DLEG regarding its ongoing investigative activities. As substantiated by this complaint letter, these activities are continuing to be engaged in by Media Sentry despite your department's letter informing them of their need to seek immediate licensure. Such actions constitute an intentional affront to the licensing requirements of the PDLA, a disregard of the jurisdiction of the DLEG, and a clear violation of the laws of Michigan. Accordingly, I would request that your department take immediate steps to issue a cease and desist letter to Media Sentry demanding that they cease their ongoing investigations of Michigan residents until such time as they are properly licensed by the state. Alternatively, the DLEG might consider the conduct of Media Sentry to warrant a referral for criminal enforcement by a local prosecutor.

I would appreciate it if you would provide me with a written response to this complaint along with a copy of any letters issued by your Department or enforcement actions taken against Media Sentry.

Sincerely,

*Case #162983070*

Case #162983070

c/o Attorney K. Orlando Simon

University of Michigan

Student Legal Services

23204 Michigan Union

530 South Street, #549

Ann Arbor, MI 48109

Enc.

## EXHIBIT A

Intellectual Property Protection with MediaSentry Services



Protect your investment and revenue

Home > Rights Management

Global Locations

Contact Us



Request Information



Technical Support



General Contact



Find SafeNet Partner

## Intellectual Property Protection with MediaSentry Services

SafeNet MediaSentry Services™ help software vendors monitor the continually evolving threat of software piracy and mitigate unauthorized distribution of their products. As a component of Unified Software Protection from SafeNet, MediaSentry Services provide continual intellectual property protection beyond your event horizon.

### Investigating Piracy of Intellectual Property

SafeNet continuously monitors the Internet for pirated software and copyright infringements. Using the data collected, you are able to determine the scale and scope of your piracy problem. Gaining visibility into the extent of piracy can help you formulate and adapt your strategies for securing your software and protecting your intellectual property.

MediaSentry investigation service offers the most advanced scanning techniques available to find and index pirated content on the Internet. From worldwide peering points, SafeNet identifies online piracy in real-time by monitoring online auction communities, IRC networks, newsgroups, FTP sites, peer-to-peer communities and websites.

Once our intelligent scanning agents find infringing activity, all relevant data is logged in our extensive database and routed to specified client folders. Captured information is fully accessible, searchable and reportable through our proprietary enterprise application.

### Online/P2P Interdiction for Intellectual Property Protection

MediaSentry interdiction services stem the trading of pirated content through seamless integration into popular piracy forums, effectively combating rampant online piracy. These intellectual property protection services combine a solid technology foundation with effective countermeasure techniques to

### Related Links

- Software Protection
- Sentinel RMS
- Sentinel Hardware Keys
- MediaSentry Services for Software Vendors**

### Related Documents

- IDC Analyst Connection "Third-Party License Management: A Path to Lower Costs and Higher Returns"

### Product Briefs:

- Unified Software Protection
- MediaSentry Services for Software Vendors

### Case Studies:

- Enigma Data Solutions Replaces Macrovision's FlexLM with Sentinel RMS
- Sentinel RMS Case Study: PGS
- Sentinel RMS Case Study: Elekta

### News and Events

- Webinar: "Licensing for Embedded Systems"

minimize the availability of pirated software online.

We employ research and intelligence experts who monitor the behavior of pirates seeking your products to identify countermeasure techniques that will be most successful. The MediaSentry Services proprietary technology platform then utilizes these techniques to make attempts to illegally download your content unfulfilling and frustrating. This customized approach ensures a solution that is flexible enough to adapt to evolving technologies and user patterns in order to achieve maximum results.

Our interdiction services are tightly integrated with our investigation platform, enabling close monitoring of the success of campaigns. A powerful reporting library, accessible through our enterprise application or via email, allows you to review the progress of enforcement campaigns in real-time.

#### **Early Leak Detection and Preemptive Protection of Intellectual Property**

Our Early Leak Detection Service proactively monitors piracy forums to quickly identify first leak file uploads and downloads files for investigation and source identification. Once piracy scanners have detected a potential leak, a series of automated processes are initiated that ensure an instant response from SafeNet and your intellectual property protection team. Early leak detection stems rapid proliferation across file-sharing networks in real-time.

#### **Online Auction Protection of Intellectual Property Rights**

Online auction communities, such as eBay, represent an additional threat for the distribution of pirated software and intellectual property. The complex and time-sensitive nature of online auction sites requires a sophisticated solution to facilitate the immediate identification and removal of illegal auctions. This program provides you with an effective and comprehensive platform to manage the enforcement process and execute auction takedowns in scale. Our managed services option eliminates client-driven manual review and further streamlines the enforcement process as MediaSentry auction managers become a virtual extension of your anti-piracy team.

#### **Intellectual Property Rights Management, Enforcement and Takedown**

SafeNet offers a comprehensive end-to-end case management enforcement tool to help you manage large-scale compliance takedown campaigns. Using our technology and enterprise service platform, you can create new cases for infringements found and send DMCA-compliant "Cease and Desist" notices to organizations, universities and service providers requesting the removal of infringing content. A full suite of compliance, escalation and workflow management options are available for configuration on a per-client basis. Litigation support to aid in prosecution of those who engage in illegal and unauthorized online distribution of your intellectual property is also available. **For additional Intellectual Property Protection, consider our Anti-Piracy Products Information.**

For more information, please download the MediaSentry Product Brief and

contact us about Intellectual Property Protection.

[Company](#) | [Site Map](#) | [Privacy Statement](#) | [Contact Us](#) | [Send Feedback](#) | [Terms & Conditions of Sale](#)  
© 2008 SafeNet Inc. All rights reserved. | Use of this website signifies your agreement to the [Terms of Use](#)

URL: [http://www.safenet-inc.com/products/sentinel/mediasentry\\_intellectual\\_property\\_protection.asp](http://www.safenet-inc.com/products/sentinel/mediasentry_intellectual_property_protection.asp) (5/12/08, font changed for instances of terms “investigating” and “investigation”)

## Intellectual Property Protection with MediaSentry Services

SafeNet MediaSentry Services™ help software vendors monitor the continually evolving threat of software piracy and mitigate unauthorized distribution of their products. As a component of Unified Software Protection from SafeNet, MediaSentry Services provide continual intellectual property protection beyond your event horizon.

### Investigating Piracy of Intellectual Property

SafeNet continuously monitors the Internet for pirated software and copyright infringements. Using the data collected, you are able to determine the scale and scope of your piracy problem. Gaining visibility into the extent of piracy can help you formulate and adapt your strategies for securing your software and protecting your intellectual property.

MediaSentry investigation service offers the most advanced scanning techniques available to find and index pirated content on the Internet. From worldwide peering points, SafeNet identifies online piracy in real-time by monitoring online auction communities, IRC networks, newsgroups, FTP sites, peer-to-peer communities and websites.

Once our intelligent scanning agents find infringing activity, all relevant data is logged in our extensive database and routed to specified client folders. Captured information is fully accessible, searchable and reportable through our proprietary enterprise application.

### Online/P2P Interdiction for Intellectual Property Protection

MediaSentry interdiction services stem the trading of pirated content through seamless integration into popular piracy forums, effectively combating rampant online piracy. These intellectual property protection services combine a solid technology foundation with effective countermeasure techniques to minimize the availability of pirated software online.

We employ research and intelligence experts who monitor the behavior of pirates seeking your products to identify countermeasure techniques that will be most successful. The MediaSentry Services proprietary technology platform then utilizes these techniques to make attempts to illegally download your content unfulfilling and frustrating. This customized approach ensures a solution that is flexible enough to adapt to evolving technologies and user patterns in order to achieve maximum results.

Our interdiction services are tightly integrated with our investigation platform, enabling close monitoring of the success of campaigns. A powerful reporting library, accessible through our enterprise application or via email, allows you to review the progress of enforcement campaigns in real-time.

### Early Leak Detection and Preemptive Protection of Intellectual Property

Our Early Leak Detection Service proactively monitors piracy forums to quickly identify first leak file uploads and downloads files for investigation and source identification. Once piracy scanners have detected a potential leak, a series of automated processes are initiated that ensure an instant response from SafeNet and your intellectual property protection team. Early leak detection stems rapid proliferation across file-sharing networks in real-time.

### Online Auction Protection of Intellectual Property Rights

Online auction communities, such as eBay, represent an additional threat for the distribution of pirated software and intellectual property. The complex and time-sensitive nature of online auction sites requires a sophisticated solution to facilitate the immediate identification and removal of illegal auctions. This program provides you with an effective and comprehensive platform to manage the enforcement process and execute auction takedowns in scale. Our managed services option eliminates client-driven manual review and further streamlines the enforcement process as MediaSentry auction managers become a virtual extension of your anti-piracy team.

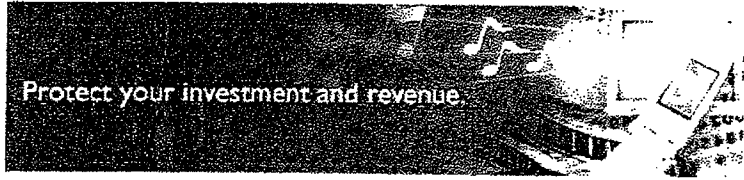
**Intellectual Property Rights Management, Enforcement and Takedown**

SafeNet offers a comprehensive end-to-end case management enforcement tool to help you manage large-scale compliance takedown campaigns. Using our technology and enterprise service platform, you can create new cases for infringements found and send DMCA-compliant "Cease and Desist" notices to organizations, universities and service providers requesting the removal of infringing content. A full suite of compliance, escalation and workflow management options are available for configuration on a per-client basis.

Litigation support to aid in prosecution of those who engage in illegal and unauthorized online distribution of your intellectual property is also available.

**For additional Intellectual Property Protection, consider our Anti-Piracy Products Information.**

For more information, please download the MediaSentry Product Brief and contact us about Intellectual Property Protection.



Global Lo

Request Information

Technical Support

General Contact

Find SafeNet Partner

### Entertainment Content Monetization

Request a copy of our report

Digital piracy is theft. Downloading a song, movie or software program for distribution without authorization is wrong and illegal. Digital piracy hurts everyone involved in the legitimate production of the goods and also hurts legitimate consumers of the material. SafeNet has extensive experience gathering evidence for civil/criminal litigation and prosecution against those who engage in unauthorized online content distribution.

to download the product brief.



Global Locations

Request Information

Technical Support

General Contact

Find SafeNet Partner

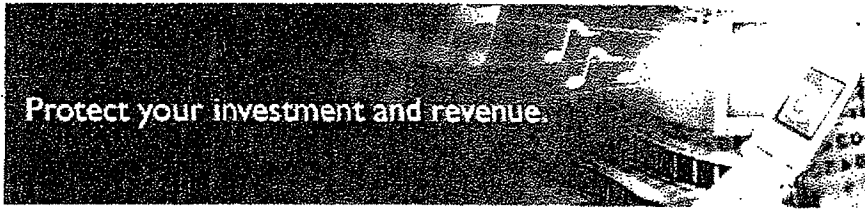
## Entertainment Content Monetization

SafeNet offers a broad suite of enforcement alternatives to meet the needs of content owners and to minimize the distribution of infringing content on the internet. Through seamless integration into popular piracy forums, our Interdiction Services stem illegal trading of copyrighted works, effectively combating rampant online piracy. MediaSentry Interdiction Services are tightly integrated with our investigation platform, allowing the success of interdiction campaigns to be closely monitored. A powerful reporting library, accessible through our enterprise application or via email, allows clients to review the progress of enforcement campaigns in real-time.

[to download the product brief](#)



Home | About Us | Contact Us | Privacy Policy | Terms of Service



Global Locations

Request Information

Technical Support

General Contact

Find SafeNet Partner

## Entertainment Content Monetization on

### Investigation Services

SafeNet continuously monitors the internet for copyright infringements. Data collected helps clients determine the scale and scope of their piracy problem and measure the success of enforcement campaigns. From worldwide peering points, SafeNet identifies online piracy in real-time by monitoring online auction communities, IRC networks, newsgroups, FTP sites, peer-to-peer communities and websites.

SafeNet believes that the data collected is most useful when it can be used to make decisions and drive changes in a strategic direction. Our Investigation Services permit clients to monitor the status of their copyright searches and create extensive management reports to track trends and the effectiveness of enforcement activity.

[Click here](#) to download the product brief.



JENNIFER M. GRANHOLM  
GOVERNOR

STATE OF MICHIGAN  
DEPARTMENT OF LABOR & ECONOMIC GROWTH  
LANSING

KEITH W. COOLEY  
DIRECTOR

February 22, 2008

Media Sentry  
4690 Mellenium Dr., Ste. 400  
Belcamp, MD 21017

RE: File No. 308967  
Complaint of Randy L. Kruger

Dear Respondent:

It has been noted during a review of the above matter by the Department of Labor & Economic Growth that you are not licensed at the address provided. You may be in violation of Section 3(1) & (2) of 1965 PA 285, MCL 338.823(1) & (2).

"338.823.amended License required; violation; penalty.

Sec. 3. (1) A person, firm, partnership, company, limited liability company, or corporation shall not engage in the business of private detective or investigator for hire, fee or reward, and shall not advertise his or her business to be that of detective or of a detective agency without first obtaining a license from the department.

(2) A person, firm, partnership, company, limited liability company, or corporation shall not engage in the business of furnishing or supplying, for hire and reward, information as to the personal character of any person or firm, or as to the character or kind of business and occupation of any person, firm, partnership, company, limited liability company, or corporation and shall not own, conduct, or maintain a bureau or agency for the purposes described in this subsection except as to the financial rating of persons, firms, partnerships, companies, limited liability companies, or corporations without having first obtained a license from the department."

Unlicensed violations are considered serious by the Department. Continuation of this practice could result in criminal prosecution. Referral of this matter may be made to the local prosecutor or police department. The prosecutor can prosecute these cases as felonies with a maximum penalty of \$5,000 and/or up to four years in prison.

If you intend to perform activities that require a private detective agency license, you must obtain a license immediately. Please call (517) 241-9288 to obtain information on how to become licensed.

If you are licensed and we do not have correct information, please notify me at the number below.

Sincerely,

Ann Paruk  
Administrative Law Specialist  
Commercial Enforcement Division  
(517) 241-9202

AP:ld

**EXHIBIT A**

**IP Address:** 141.213.250.26 2008-03-18 05:18:05 EDT

**CASE ID#** 162983070

**P2P Network:** GnutellaUS (LimeWire)

**Total Audio Files:** 529

<u>Copyright Owner</u>	<u>Artist</u>	<u>Recording Title</u>	<u>Album Title</u>	<u>SR#</u>
UMG Recordings, Inc.	Nelly	Grillz	Grillz (single)	385-148
SONY BMG MUSIC ENTERTAINMENT	Switchfoot	Meant to Live	The Beautiful Letdown	347-967
SONY BMG MUSIC ENTERTAINMENT	Mariah Carey	Someday	Mariah Carey	118-408
Capitol Records, Inc.	Coldplay	Fix You	X&Y	376-828
Virgin Records America, Inc.	Gorillaz	Feel Good Inc.	Feel Good Inc. (single)	379-134
Arista Records LLC	Outkast	Rosa Parks	Aquemini	264-092
Capitol Records, Inc.	Coldplay	Yellow	Parachutes	328-762
London-Sire Records Inc.	Eden's Crush	Get Over Yourself	Popstars	187-319
UMG Recordings, Inc.	Nelly Furtado	Say It Right	Loose	387-509

**EXHIBIT A**

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF MICHIGAN  
NORTHERN DIVISION

LAFACE RECORDS LLC, a Delaware limited liability company; ARISTA RECORDS LLC, a Delaware limited liability company; ATLANTIC RECORDING CORPORATION, a Delaware corporation; BMG MUSIC, a New York general partnership; CAPITOL RECORDS, LLC, a Delaware limited liability company; ELEKTRA ENTERTAINMENT GROUP INC., a Delaware corporation; INTERSCOPE RECORDS, a California general partnership; LAVA RECORDS LLC, a Delaware limited liability company; MAVERICK RECORDING COMPANY, a California joint venture; SONY BMG MUSIC ENTERTAINMENT, a Delaware general partnership; UMG RECORDINGS, INC., a Delaware corporation; VIRGIN RECORDS AMERICA, INC., a California corporation; WARNER BROS. RECORDS INC., a Delaware corporation; and ZOMBA RECORDING LLC, a Delaware limited liability company,

Hon. :  
Case :

Plaintiffs,

v.

DOES 1 - 21,

Defendants.

---

JASON R. GOURLEY (P69065)  
MATTHEW E. KRICHBAUM (P52491)  
SOBLE ROWE KRICHBAUM, LLP  
Attorneys for Plaintiffs  
221 North Main Street, Suite 200  
Ann Arbor, Michigan 48104  
(734) 996 5600

---

**DECLARATION OF CARLOS LINARES IN SUPPORT OF APPLICATION FOR  
LEAVE TO TAKE IMMEDIATE DISCOVERY**

I, Carlos Linares, have personal knowledge of the facts stated below and, under penalty of perjury, hereby declare:

1. I am an attorney and Vice President, Anti-Piracy Legal Affairs for the Recording Industry Association of America, Inc. ("RIAA"), where I have been employed for over six years. My office is located at 1025 F Street, N.W., 10<sup>th</sup> Floor, Washington, DC 20004. I submit this Declaration in support of Plaintiffs' *Ex Parte* Application for Leave to Take Immediate Discovery.

2. As Vice President, Anti-Piracy Legal Affairs, I am responsible for evaluating and contributing to online strategies for the RIAA and its member record companies who are Plaintiffs in this action, including oversight of the investigations into online infringement of copyrighted sound recordings. As such, this Declaration is based on my personal knowledge, and if called upon to do so, I would be prepared to testify as to its truth and accuracy.

**The RIAA's Role in Protecting Its Member Recording Industry Companies From  
Copyright Infringement**

3. The RIAA is a not-for-profit trade association whose member record companies create, manufacture, and/or distribute approximately ninety percent of all legitimate sound recordings produced and sold in the United States. The RIAA's member record companies comprise the most vibrant national music industry in the world. A critical part of the RIAA's mission is to assist its member companies in protecting their intellectual property in the

United States and in fighting against online and other forms of piracy. All of the Plaintiffs in this action are members of the RIAA.

4. As part of that process, the RIAA, on behalf of its members, retains a variety of services from outside vendors to assist with its investigation of the unauthorized reproduction and distribution of copyrighted sound recordings online.

#### **The Internet and Music Piracy**

5. The Internet is a vast collection of interconnected computers and computer networks that communicate with each other. It allows hundreds of millions of people around the world to communicate freely and easily and to exchange ideas and information, including academic research, literary works, financial data, music, movies, graphics, and an unending and ever-changing array of other data. Unfortunately, the Internet also has afforded opportunities for the wide-scale piracy of copyrighted sound recordings and musical compositions. Once a sound recording has been transformed into an unsecured digital format, it can be copied further and distributed an unlimited number of times over the Internet, without significant degradation in sound quality.

6. Much of the unlawful distribution of copyrighted sound recordings over the Internet occurs via "peer-to-peer" ("P2P") file copying networks or so-called online media distribution systems. The most notorious example of such a system was Napster, which was enjoined by a federal court. Notwithstanding the court's decision enjoining Napster, similar online media distribution systems emerged and attempted to capitalize on the growing illegal market that Napster fostered. These include KaZaA, eDonkey, iMesh, Ares, BitTorrent, DirectConnect, and Gnutella, among others. To this day, some P2P networks continue to operate and to facilitate widespread copyright piracy. At any given moment, millions of people illegally use online media distribution systems to upload or download copyrighted material.

7. P2P networks, at least in their most popular form, refer to computer systems or processes that enable Internet users to: (1) index files (including audio recordings) into a share directory on a computer that are then searched for and transferred to other users; (2) search for files stored on other users' computers; (3) transfer exact copies of files from one computer to another via the Internet; and (4) allow users to further distribute the files to other users. P2P networks enable users who otherwise would have no connection with, or knowledge of, each other to offer to each other for distribution and copying files off of their personal computers, to provide a sophisticated search mechanism by which users can locate these files for downloading, and to provide a means of effecting downloads.

8. The major record companies generally have not authorized their copyrighted sound recordings to be copied or distributed in unsecured formats by means of P2P networks. Thus, the vast majority of the content that is copied and distributed on P2P networks is unauthorized by the copyright owner – that is, the distribution violates the copyright laws.

9. The scope of online piracy of copyrighted works cannot be underestimated. The RIAA member companies lose significant revenues on an annual basis due to the millions of unauthorized downloads and uploads of well-known recordings that are distributed on P2P networks by infringers who, in virtually all cases, have the ability to maintain their anonymity to all but the Internet Service Provider (“ISP”) they use to supply them with access to the Internet.

10. The persons who commit infringements by using the P2P networks are, by and large, anonymous to Plaintiffs. A person who logs on to a P2P network is free to use any alias (or computer name) whatsoever, without revealing his or her true identity to other users.

Thus, Plaintiffs can observe the infringement occurring on the Internet, but do not know the true names or mailing addresses of those individuals who are committing the infringement.

**The RIAA's Identification of Copyright Infringers**

11. In order to assist its members in combating copyright piracy, the RIAA retained a third-party investigator, MediaSentry, Inc. ("MediaSentry"), to conduct searches of the Internet, as well as file-copying services, for infringing copies of sound recordings whose copyrights are owned by RIAA members. A search can be as simple as logging onto a P2P network and examining files being distributed by others logged onto the network. In gathering evidence of copyright infringement, MediaSentry uses the same functionalities that are built into P2P programs that any user of the software can use on the network.

12. Users of P2P networks who distribute files over a network can be identified by using Internet Protocol ("IP") addresses because the unique IP address of the computer offering the files for distribution can be captured by another user during a search or a file transfer. Users of P2P networks can be identified by their IP addresses because each computer or network device (such as a router) that connects to a P2P network must have a unique IP address within the Internet to deliver files from one computer or network device to another. Two computers cannot effectively function if they are connected to the Internet with the same IP address at the same time. In some cases, more than one computer can access the internet over a single IP address by using network address translation, in which cases the computer port being used provides further identification of the computer engaged in the on-line communication. This is analogous to the telephone system where each location has a unique number (and the port acts much like a specific telephone extension off the main switch board). For example, in a particular home, there may be three or four different telephones, but only one call can be placed at a time to or from that home. Each computer or network device is connected

to a network that is administered by an organization like a business, ISP, college, or university. Each network, in turn, is analogous to an area code. The network provider maintains a log of IP address allocations. An IP address can be associated with an organization such as an ISP, business, college, or university, and that organization can identify the P2P network user associated with the specified IP address.

13. MediaSentry finds individuals using P2P networks to share music files over the Internet. Just as any other user on the same P2P networks as these individuals would be able to do, MediaSentry is able to detect the infringement of copyrighted works and identify the users' IP addresses because the P2P software being used by those individuals has file-sharing features enabled.

14. For each suspected infringer, MediaSentry downloads a number of the music files that the individual is offering to other users on the P2P network. Those music files for each such individual are listed in Exhibit A to the Complaint. MediaSentry assigns an identification number to each individual for which it detects copyright infringement and gathers additional evidence for each individual, such as metadata accompanying each file being disseminated that demonstrates that the user is engaged in copyright infringement. That evidence includes download data files that show for each music file the source IP address, user logs that include a complete listing of all files in the individual's share folder at the time, and additional data that track the movement of the files through the Internet.

15. After MediaSentry collects the evidence of infringement, the RIAA engages in a painstaking process to verify whether each individual was infringing. That process relies on human review of evidence supporting the allegation of infringement. For each suspected infringer, the RIAA reviews a listing of the music files that the user has offered for

download by others from his or her computer in order to determine whether they appear to be copyrighted sound recordings. The RIAA also listens to the downloaded music files from these users in order to confirm that they are, indeed, copies of sound recordings whose copyrights are owned by RIAA members. Exhibit A to the Complaint lists the details of these downloaded music files. In my role as Vice President, Anti-Piracy, I provide oversight over the review of the lists contained in Exhibit A to the Complaint and hereby attest to the veracity of those lists. The RIAA also reviews the other evidence collected by MediaSentry.

**The Subpoena Process to Identify Copyright Infringers**

16. The RIAA frequently has used the subpoena processes of Federal Rule of Civil Procedure 45 to obtain the names of infringers from ISPs. The RIAA typically has included in their subpoenas to ISPs an IP address and a date and time on which the RIAA, through its agent, MediaSentry, observed use of the IP address in connection with allegedly infringing activity. In some instances, providing the IP address alone to the ISP has been enough to enable the ISP to identify the infringer. Providing the date and time further assists some ISPs in identifying infringers, especially ISPs that use “dynamic IP addressing” such that a single computer may be assigned different IP addresses at different times, including, for example, each time it logs into the Internet.<sup>1</sup> Some ISPs also ask for the computer port information to further identify the infringer. Once provided with the IP address, plus the date and time of the infringing activity, the infringer’s ISP can typically identify the computer from which the infringement occurred (and the name and address of the subscriber that controls that computer), sometimes within a matter of minutes.

---

<sup>1</sup> ISPs own or are assigned certain blocks or ranges of IP addresses. An ISP assigns a particular IP address in its block or range to a subscriber when that subscriber goes “online.”

17. Since 1998, the RIAA and others have used subpoenas thousands of times to learn the names, addresses, telephone numbers, and e-mail addresses of infringers for the purpose of bringing legal actions against those infringers.

**The RIAA's Identification of the Infringers in This Case**

18. In the ordinary course of investigating online copyright infringement, the RIAA became aware that Defendants were distributing files to others on various P2P networks. The user-defined author and title of the files being distributed by each Defendant suggested that many were copyrighted sound recordings being disseminated without the authorization of the copyright owners. The RIAA downloaded and listened to a representative sample of the music files being distributed by each Defendant and was able to confirm that the files each Defendant was distributing were illegal copies of sound recordings whose copyrights are owned by RIAA members. The RIAA also recorded the time and date at which the infringing activity was observed and the IP address assigned to each Defendant at the time. See Complaint Exhibit A. The RIAA could not, however, determine the physical location of the users or their identities. The RIAA could determine that Defendants were all using Central Michigan University internet service to distribute the copyrighted files.

19. The RIAA also has collected for each Defendant a list of the files each Defendant was distributing to the public. These lists often show thousands of files, many of which are sound recording (MP3) files that are owned by, or exclusively licensed to, Plaintiffs. Because of the voluminous nature of the lists, and in an effort not to overburden the Court with paper, I have not attached to this Declaration those lists. Such lists will be made available to the Court upon request. Exhibit A to the Complaint includes the username of the infringer if that was available, the identification number assigned by MediaSentry for that Defendant, and the

number of audio files that were being shared by Defendant at the time that the RIAA's agent, MediaSentry, observed the infringing activity.

**The Importance of Expedited Discovery in This Case**

20. Obtaining the identity of copyright infringers on an expedited basis is critical to stopping the piracy of the RIAA members' copyrighted works.

21. First, every day that copyrighted material is disseminated without the authorization of the copyright owner, the copyright owner is economically harmed. Prompt identification of infringers is necessary in order for copyright owners to take quick action to stop unlawful dissemination of their works and minimize their economic losses.

22. Second, infringement often occurs with respect to sound recordings that have not yet been distributed publicly. Such infringement inflicts great harm on the initial market for new works. New recordings generally earn a significant portion of their revenue when they are first released, and copyright piracy during a recording's pre-release or early release period therefore deprives copyright owners of an important opportunity to reap the benefits of their labor.

23. Third, without expedited discovery, Plaintiffs have no way of serving Defendants with the complaint and summons in this case. Infringement occurs without name tags so Plaintiffs do not have Defendants' names or addresses, nor do they have an e-mail address for Defendants.

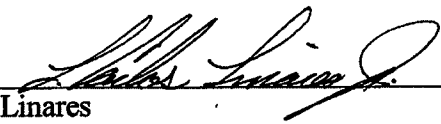
24. Fourth, computer evidence by its very nature is subject to being overwritten. At times, Plaintiffs have sought evidence from defendants' computers only to find that the evidence of infringement was destroyed (intentionally or unintentionally). Expedited discovery is critical to allow Plaintiffs to put Defendants on notice of the need to preserve the electronic evidence and avoid the loss of evidence.

25. Fifth, ISPs have different policies pertaining to the length of time they preserve “logs” which identify their users. ISPs keep log files of their user activities for only limited periods of time – which can range from as short as a few days, to a few months – before erasing or overwriting the data they maintain. If an ISP does not respond expeditiously to a discovery request, the identification information in the ISP’s logs may be erased, making it impossible for the ISP to determine the identity of the infringer and eliminating the copyright owner’s ability to take action to stop the infringement. The RIAA notifies the ISPs when it has identified infringement for which it will seek identifying information and requests the ISPs to preserve the information. In most cases the ISPs preserve at least some of the information necessary to identify the infringer, but not always. Some ISPs have indicated they will preserve the information for a limited time.

*[Remainder of page intentionally left blank.]*

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

Executed on May 23, 2008 in Washington, D.C.

  
\_\_\_\_\_  
Carlos Linares

**EXHIBIT A**

**Doe # 1** IP Address: 141.209.107.165 2008-03-16 17:46:47 EDT  
Case ID: 162796121

**Doe # 2** IP Address: 141.209.109.187 2008-03-18 19:37:14 EDT  
Case ID: 163047200

**Doe # 3** IP Address: 141.209.109.232 2007-11-08 18:32:31 EST  
Case ID: 147314928

**Doe # 4** IP Address: 141.209.134.205 2007-12-01 00:54:39 EST  
Case ID: 149940528

**Doe # 5** IP Address: 141.209.192.227 2007-11-12 06:28:05 EST  
Case ID: 147632392

**Doe # 6** IP Address: 141.209.192.30 2008-02-06 15:57:54 EST  
Case ID: 158272830

**Doe # 7** IP Address: 141.209.196.67 2008-02-12 03:57:53 EST  
Case ID: 158872490

**Doe # 8** IP Address: 141.209.200.6 2007-11-15 16:54:09 EST  
Case ID: 147971404

**Doe # 9** IP Address: 141.209.202.93 2007-11-18 10:53:00 EST  
Case ID: 148268514

**Doe # 10** IP Address: 141.209.204.153 2008-03-24 12:24:47 EDT  
Case ID: 163748224

**Doe # 11** IP Address: 141.209.218.136 2008-03-14 05:34:40 EDT  
Case ID: 162491211

**Doe # 12** IP Address: 141.209.223.226 2008-03-29 20:45:39 EDT  
Case ID: 164460491

**Doe # 13** IP Address: 141.209.231.40 2008-03-24 19:00:38 EDT  
Case ID: 163778858

**Doe # 14** IP Address: 141.209.237.181 2007-12-12 00:06:21 EST  
Case ID: 151455321

**Doe # 15** IP Address: 141.209.239.201 2008-02-24 17:30:41 EST  
Case ID: 160323217

**Doe # 16** IP Address: 141.209.47.63 2007-11-15 03:15:26 EST  
Case ID: 147906915

**Doe # 17** IP Address: 141.209.51.249 2008-02-13 11:21:58 EST  
Case ID: 159009972

**Doe # 18** IP Address: 141.209.52.155 2007-12-13 19:48:14 EST  
Case ID: 151695707

**Doe # 19** IP Address: 141.209.52.91 2008-02-13 02:42:24 EST  
Case ID: 158973373

**Doe # 20** IP Address: 141.209.65.112 2007-11-13 14:40:23 EST  
Case ID: 147754652

**Doe # 21** IP Address: 141.209.85.173 2007-11-17 13:33:08 EST  
Case ID: 148171764



JOHN ELIAS BALDACCI  
GOVERNOR  
ANNE H. JORDAN  
COMMISSIONER

STATE OF MAINE  
*Department of Public Safety*  
*Maine State Police*  
*Special Investigations*  
164 State House Station  
Augusta, Maine  
04333



COL. PATRICK J. FLEMING  
LT. COL. ROBERT A. WILLIAMS  
DEPUTY CHIEF

Thursday, April 10, 2008

MediaSentry, Inc.  
4690 Millennium Drive  
Belcamp, MD 21017

To Whom It May Concern:

It has been brought to my attention that your business is conducting investigations for the RIAA in Maine. My records indicate that you are not licensed in Maine to conduct Private Investigator business. Maine statute Title 32, Chapter 89, subsection 8103.5 Defines a Private Investigator as "any person who, for any consideration whatsoever, engages in or solicits business or accepts employment to furnish, or agrees to make or makes any investigation to obtain information with reference to any of the following:

- A. Any crime or other committed or threatened against the laws or government of the United States, any state or territory, or any political subdivision thereof;
- B. The identity, habits, conduct, movements, whereabouts, affiliations, associations, transactions, reputation or character of any person;
- C. Libels, fires, losses, accidents, or damage or injury to persons or property;
- D. The location, disposition or recovery of lost or stolen property; or
- E. Evidence to be used before any court, board, officer or investigative committee.

As referred to on you web page, you meet the criteria of a Private Investigator. Title 32, Chapter 89, Subsection 8104 states "No person may act as a private investigator without first obtaining from the commissioner a license to be a private investigator or investigative assistant." Therefore it would be illegal to continue acting in the capacity of a Private Investigator in Maine unless licensed. Please contact me with any questions or information that would clarify my understanding of this situation.

CC: SafeNet Corporate Headquarters

Respectfully,

Detective David Pelletier  
Maine State Police  
Special Investigations Unit  
(207) 624-7076



DEVAL L. PATRICK  
GOVERNOR

TIMOTHY R. MURPHY  
LIEUTENANT GOVERNOR

KEVIN N. BUNKE  
SECRETARY

COLONEL MARK H. DELANEY  
SUPERINTENDENT

# The Commonwealth of Massachusetts Department of State Police

Certification Unit

235 North Street

Danvers, MA 01923

(978) 538-6128 Voice - (978) 538-6021 Fax

January 2, 2008

Mr. Chris Steven Fedde, Jr.  
Safenet, Inc.  
4690 Millenium Drive  
Belcamp, MD 21017

Mr. Fedde:

An investigation by this office has revealed that you are advertising and operating a Private Detective company under the title of "Safenet, Inc." and "MediaSentry". A review of our records indicates that you are not licensed to conduct investigations in the Commonwealth of Massachusetts under this business name.

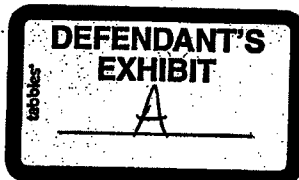
This is an official cease and desist order. Your company is not licensed to advertise or perform the business of Private Investigations in the Commonwealth of Massachusetts. You are in violation of MGL Chapter 147, Sections 22 and 23. If further inquiries prove that you are currently operating or advertising without a license complaints for violation of this statute will be forthcoming.

Specifically, MGL Chapter 147, Section 23 states that "No person shall engage in, advertise or hold himself out as being engaged in, nor solicit private detective business or the business of watch, guard or patrol agency, notwithstanding the name or title used in describing such business, unless licensed for such purpose as provided in section twenty-five". Section 23 also states, "Whoever violates any provision of this section shall be punished by a fine of not less than two hundred nor more than one thousand dollars or by imprisonment for not more than one year, or by both such fine and imprisonment".

If you have any questions or concerns, please contact me at the above telephone number.

Regards,

*Sgt. Chester Bishop*  
Sergeant Chester Bishop  
Certification Unit



*Excellence In Service Through Quality Policing*