**UNITED STATES DISTRICT COURT**
**DISTRICT OF MASSACHUSETTS**

| | |
|---|---|
| **CAPITOL RECORDS, INC.**, *et al.*,<br><br>*Plaintiffs*,<br><br>v.<br><br>**NOOR ALAUJAN**,<br><br>*Defendant*. | Civ. Act. No. 03-cv-11661-NG<br>(LEAD DOCKET NUMBER) |
| **SONY BMG MUSIC ENTERTAINMENT**, *et al.*,<br><br>*Plaintiffs*,<br><br>v.<br><br>**JOEL TENENBAUM**,<br><br>*Defendants*. | Civ. Act. No. 1:07-cv-11446-NG<br>(ORIGINAL DOCKET NUMBER) |

**MOTION TO SUPPRESS EVIDENCE**

Charles R. Nesson
1575 Massachusetts Avenue
Cambridge, MA 02138
617-495-4609
nesson@law.harvard.edu

K.A.D. Camara
Camara & Sibley LLP
2339 University Boulevard
Houston, Texas 77005
713-893-7973
713-583-1131 (fax)
camara@camarasibley.com

*Attorneys for Defendant Joel Tenenbaum*

Dated: June 23, 2009

**MOTION TO SUPPRESS**

The recording industry's only evidence that Joel Tenenbaum ever downloaded or shared music on KaZaA is the evidence collected by MediaSentry. MediaSentry collected this evidence in violation of federal and state criminal statutes that restrict wiretapping and require that private detectives be trained and licensed. It collected this evidence at the direction and under the supervision of lawyers for the recording industry, including opposing counsel in this case. These same lawyers have used MediaSentry evidence to fuel not only this prosecution, but also their entire five-year campaign against tens of thousands accused of sharing music online — a litigation campaign that has earned their recording-industry clients more than $100 million in settlements.

In orchestrating this campaign, built around illegally obtained evidence and targeted at individuals, most of whom faced millions of dollars of potential liability without the assistance of counsel, these lawyers violated the ethical rules governing our profession on an unprecedented scale. We respectfully request that this Court remedy this ethical violation by suppressing all MediaSentry evidence in this case. In the first recording-industry prosecution to go to trial, the jury returned a verdict of $1.92M, or $80,000 per song for 24 songs. We submit that, with stakes this high, the federal courts should make clear to the world that the kind of gross abuse of federal process that we have seen in the last seven years will never again be permitted.

If this Court grants our motion to suppress, we anticipate moving for a directed verdict for Joel Tenenbaum on all claims.

## I. MEDIASENTRY COLLECTED ITS EVIDENCE AGAINST JOEL TENENBAUM IN VIOLATION OF FEDERAL AND STATE CRIMINAL LAW.

MediaSentry collected the evidence against Joel Tenenbaum in violation of the Massachusetts Private Detectives Act, M.G.L. 147 § 22 *et seq.*; the federal Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 *et seq.* ("Wiretap Act"); and the Massachusetts Wiretapping Statute, M.G.L. 272 § 99. *See generally* Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 Nw. U. L. Rev. 607 (2003). These violations were crimes under federal and state law.

### A. The Evidence Against Joel Tenenbaum

The only evidence that Joel Tenenbaum downloaded or distributed music online is the dossier compiled by MediaSentry about Joel's alleged use of KaZaA and the testimony of its representative, Mark Weaver.[1]

The RIAA and MediaSentry used KaZaA to seek out and identify users who share copyrighted sound recordings. KaZaA is a peer-to-peer file-sharing program used by millions of people worldwide to share files. KaZaA is actually one of a family of programs that interconnect using a peer-to-peer technology known as FastTrack. Peer-to-peer file-sharing systems, including those based on FastTrack, allow a user to search for files that are available from other users of the system, and to selectively download files that are found as a result of this search.

The MediaSentry investigation proceeds as follows. MediaSentry, using its own copy of KaZaA, searches the KaZaA network for files with names that suggest sound recordings for which the recording companies own or hold license to the copyrights.

[1] Most of this evidence is inadmissible for other reasons under the Federal Rules of Evidence. By describing this evidence here, we do not waive our objections submitted now or that we may raise at trial.

When MediaSentry finds these files, it connects to the KaZaA instance running on the machine that is offering these files for download. Through the KaZaA interface, MediaSentry then lists all the files available on the remote machine. The KaZaA interface displays information about each file available. MediaSentry records an image for each screen displayed by KaZaA when it lists the available files. Finally, MediaSentry, using KaZaA, downloads selected files — but not all of them or even all on which the RIAA later decides to sue — to their own machine to confirm that the files are in fact copyrighted sound recordings.

While running KaZaA, MediaSentry also utilizes a separate process to capture every packet of information that is sent between their instance of KaZaA and any other remote instance of KaZaA. In effect, MediaSentry monitors or taps into the network traffic between its instance of KaZaA and other instances of KaZaA. This eavesdropping provides additional information to MediaSentry. The information that MediaSentry obtains in this way is not visible through the ordinary user interface of KaZaA. It is part of the internal workings of KaZaA and the Internet, part of the process of sending information between KaZaA instances.

MediaSentry is able to determine the IP addresses of other KaZaA users' machines through this process. Information on the Internet is exchanged in discrete chunks called 'packets.' *U.S. v. Councilman* 418 F.3d 67 (1st Cir. 2005) (describing delivery of packets in context of email system). Like a mailing envelope, each packet has a sender and a recipient address. These addresses are in a special format consisting of four numbers (e.g. 128.0.0.1) and are known as IPv4 ("IP"), or Internet Protocol Version 4, addresses. *See* http://www.iana.org/numbers/. Many also compare IP

addresses to phone numbers. These IP addresses are then used in the subpoena process to determine the names and addresses of persons who are associated with the accounts to which the IP addresses were assigned on the dates and times of intercept by MediaSentry.

MediaSentry found Joel's computer by (1) using KaZaA to request a file transfer from Joel's computer to a MediaSentry computer; (2) using a separate program or programs to intercept the Internet packets being sent from Joel's computer to the MediaSentry computer as a result of this request; (3) reading the IP address of Joel's computer from these packets; and (4) tracing this IP address back to Joel. This kind of investigation of network traffic is lawful only if certain procedures are followed: when there is prior approval by a court and when the person conducting the investigation is properly licensed. When these procedures are not followed, such investigation constitutes criminal wiretapping and the illegal collection of evidence by an unlicensed private detective.

**B. Massachusetts Private Detectives Act**

MediaSentry collected evidence in violation of the Massachusetts Private Detectives Act, M.G.L. 147 § 22 *et seq*. The Massachusetts Department of State Police concluded that MediaSentry was violating the Private Detectives Act and sent a letter to MediaSentry putting it on notice of this violation in January 2008. *See* Ex. A. We are in the process of obtaining the State Police's file on MediaSentry and will present this to the Court as a supplementary exhibit as soon as we are able to obtain it. In any event, MediaSentry's violation of the Private Detectives Act is apparent simply from reading the Act's text.

The Private Detectives Act makes it a crime to carry on the business of a private detective without a license from Massachusetts:

> **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.
>
> * * *
>
> 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.

M.G.L. 147 § 23 (emphasis added). Neither MediaSentry nor any of its employees were licensed private detectives in Massachusetts.

It is the business of a private detective, as defined by the Private Detectives Act, to "make[] investigations for the purpose of obtaining . . . [e]vidence to be used . . . in the trial of civil or criminal cases." M.G.L. 147 § 22. The definitions section of the Act provides:

> "Private detective business", the business of private detective or private investigator, and the business of watch, guard or patrol agency.
>
> "Private detective" or "private investigator", a person engaged in business as a private detective or private investigator, including **any person who, for hire, fee, reward or other consideration**, (1) uses a lie-detector for the purpose of obtaining information with reference to the conduct, integrity, efficiency, loyalty or activities of any person or (2) **engages in the business of making investigations for the purpose of obtaining information with reference to any of the following matters**, whether or not other functions or services are also performed for hire, fee, reward or other consideration, or other persons are employed to assist in making such investigations:--
>
> > (a) Crime or other acts committed or threatened against the laws or government of the United States or any state of the United States;

> (b) The identity, habits, conduct, movements, whereabouts, affiliations, associations, transactions, reputation or character of any person;
>
> (c) Libels, fires, losses, accidents, or damage to, or loss or theft of, real or personal property;
>
> (d) **Evidence to be used** before any investigating committee, board of award, or board of arbitration, or **in the trial of civil or criminal cases.**

M.G.L. 147 § 22 (emphasis added). MediaSentry was engaged in the business of a private detective because, as its business and for a fee paid by the recording industry, it collected evidence to be used against defendants like Joel Tenenbaum in civil trials like the imminent trial in this case.

The requirement of a license advances at least two policies, manifested in the requirements for licensure set out in the Act. MediaSentry could not have met these requirements had it sought a license in Massachusetts. First, a licensee must be known well by three citizens of the locality in which the licensee proposes to be a private investigator. An application:

> shall include a certification by each of three reputable citizens of the commonwealth residing in the community in which the applicant resides or has a place of business, or in which the applicant proposes to conduct his business, that he has personally known the applicant for at least three years, that he has read the application and believes each of the statements made therein to be true, that he is not related to the applicant by blood or marriage, and that the applicant is honest and of good moral character.

M.G.L. 147 § 24. This ensures that investigators are subject to local censure and are sensitive to the privacy interests of those around whom they work.

Second, a licensee must have substantial training in law enforcement: years of service with a law-enforcement agency.

> The applicant . . . shall have been regularly employed for not less than three years as a detective doing investigating work, a former member of an

> investigative service of the United States, a former police officer, of a rank or grade higher than that of patrolman, of the commonwealth, any political subdivision thereof or an official police department of another state, or a police officer in good standing formerly employed for not less than ten years with the commonwealth, or any political subdivision thereof or with an official police department of another state.

M.G.L. § 147 § 24. This requirement ensures that investigators are not only technically competent, but also are familiar with the practices of professional private investigators, including those related to complying with laws governing investigation, such as the state and federal Wiretap Acts.

The policies underlying licensing statutes for private investigators have particular application in the context of peer-to-peer file-sharing networks like KaZaA. Inadvertent file sharing on these networks is common. Professor Eric Johnson of Dartmouth, in a recent study presented to the House Committee on Oversight and Government Reform, found sensitive medical records, social security numbers, and other personal information — files that no user would have shared intentionally — available from users' computers on peer-to-peer networks. Congress has launched investigations into the possible national-security consequences of inadvertent file sharing after a series of high-profile leaks of confidential documents. The leaked documents include the blueprints and avionics for Marine One, the President's helicopter; more than 150,000 tax returns, 25,800 student-loan applications, 626,000 credit reports, and the investment file of Justice Stephen Breyer.

Licensing statutes like the Private Detective Act are an important tool of state law for preventing unauthorized persons from accessing inadvertently shared information like this. They represent a decision by the state that citizens' interest in privacy is more important than their interest in being able to engage companies like MediaSentry to

detect private wrongs or even public crimes. And they are widespread: MediaSentry violated the Private Detectives Act not only of Massachusetts, but of almost every state in the Union. In particular, Maryland and New Jersey, the two states in which MediaSentry claims to have been operating when it investigated Joel in Massachusetts both have Detectives Acts analogous to the Massachusetts Act. *See* N.J. Stat. §§ 45:19, 2A:156A-2; Md. Code, Business Occupations & Professions § 13-801; Md. Code, Courts & Judicial Proceedings § 10-402. Rhode Island also has a parallel Detectives Act that MediaSentry violated. *See* R.I. Stat. § 5-5-1 *et seq.* (§ 5-5-2 defining *private detective* as "a person who is hired for the purpose of conducting investigations involving . . . (ii) Clandestine surveillance; . . . (iv) The search for lost or stolen property").

**C. Electronic Communications Privacy Act of 1986**

MediaSentry's activities also violated the federal Wiretap Act, 18 U.S.C. § 2510 *et seq.* The Wiretap Act broadly prohibits wiretapping:

> Except as otherwise specifically provided in this chapter, **any person who** —
>
> > (a) **intentionally intercepts**, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, **any** wire, oral, or **electronic communication**;
> >
> > .* * *
> >
> > (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; [or]
> >
> > (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection,

> **shall be punished** as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

18 U.S.C. § 2511(1) (emphasis added).

MediaSentry violated § 2511(1) by intercepting electronic communications, namely, the packets traveling between the KaZaA instances on the computers being used by MediaSentry and Joel. The Wiretap Act defines *intercept* as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). The information in these IP packets, including, critically, the IP address associated with Joel's machine, was not visible through the user interface of KaZaA. Accessing this information required going behind KaZaA — behind the visible. public part of the electronic communications at issue — to the underlying IP packets being sent over the Internet. It required tapping the net. *See also O'Brien v. O'Brien,* 899 So.2d 1133 (Fla.App. 5 Dist. 2005) (recorded screenshots constitute interception of electronic communications).

MediaSentry does not fall within any of the exceptions to the Wiretap Act. The exceptions that come closest to applying are those in 18 U.S.C. § 2511(2)(d) and 18 U.S.C. § 2511(2)(g)(1). Section 2511(2)(d) provides:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

18 U.S.C. § 2511(2)(d). This section permits interception of an electronic communication where one party to the communication, here, MediaSentry, consents, but only if the interception is not done "for the purpose of committing any criminal or

tortious act in violation of the Constitution or laws of the United States or of any State." *Id*.

Section 2511(2)(d) does not protect MediaSentry because MediaSentry was intercepting communications for the purpose of committing the crime under Massachusetts law of engaging in the business of a private detective without a license. MediaSentry was also violating the Massachusetts Wiretap Statute, which requires consent by both parties for recording, not merely consent by one party. *See* M.G.L. 272 § 99. *See also Sussman v. American Broadcasting Companies, Inc.*, 186 F.3d 1200 (9th. Cir 1999) (noting exception to single-party consent where purpose of tap is criminal act); *U.S. v. Lam*, 271 F. Supp. 2d 1182 (N.D. Cal. 2003) (recordings bookie made of his own phone calls for the criminal purpose of keeping records of his gambling operation held to violate Wiretap Act).

MediaSentry also does not qualify for the exception in § 2511(2)(g)(i). That section provides:

> It shall not be unlawful under this chapter or chapter 121 of this title for any person — (i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public

18 U.S.C. § 2511(2)(g)(i). This section does not apply because the KaZaA network is available only to users of KaZaA who consent to certain terms of use, not to the general public. Further, KaZaA encrypts the information it sends between different nodes, and that information is not generally visible or available to the public. Thus, the electronic communications over the KaZaA network that MediaSentry monitored were not "readily accessible to the general public."

The Senate Report accompanying enactment of § 2511(2)(g)(i) explains that whether an electronic communication is readily accessible depends on whether the public is freely authorized to access the electronic communication. *See* S. Rep. 99-541, 1986 U.S.C.C.A.N. 3555, 3590 (1986). It explains that a service is generally accessible if it "does not require any special access code or warning to indicate that the information is private." KaZaA requires both these things: it requires a username and password to log on to the network and decode the encrypted communications, and such a username and password can be obtained only by signing on to certain terms of use that give notice that the electronic communications on the network are private.

The KaZaA terms of use forbid exactly what MediaSentry did in this case: (1) making requests to gather information about other users; (2) storing information about other users; (3) violating state and federal laws; (4) developing and deploying separate software to monitor the network; and (5) altering data stored by KaZaA on MediaSentry's computer. Specifically, MediaSentry violated the following terms:

> 2.11 [What You Can't Do Under This License] Monitor traffic or make search requests in order to accumulate information about individual users;
>
> 2.14 [What You Can't Do Under This License] Collect or store personal data or other information about other users;
>
> 2.9 [What You Can't Do Under This License] Interfere with or disrupt the Software;
>
> 2.10 [What You Can't Do Under This License] Intentionally or unintentionally violate any applicable local, state, national or international law, including securities exchange and any regulations requirements, procedures or policies in force from time to time relating to the Software;
>
> 3.4 You may not use, test or otherwise utilize the Software in any manner for purposes of developing or implementing any method or

> application that is intended to monitor or interfere with the functioning of the Software.
>
> 3.5 You may not through the use of any third party software application, alter or modify the values stored by the Software in your computer's memory, on your computer's hard disk, or in your computer's registry, or, with the exception of completely uninstalling the Software, otherwise modify, alter or block the functioning of the Software.

*See* Ex. F (KaZaA End User License Agreement, February 2005).

These terms of use, violated by MediaSentry, show that KaZaA was not a network containing electronic communications generally accessible to the public, but was instead a private network for communications between users who had obtained special usernames and passwords and who consented to certain restrictive terms and conditions. *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 875 (9th Cir. 2002) ("Congress wanted to protect electronic communications that are configured to be private."). Moreover, KaZaA encrypts communications on its network to preserve privacy. *Cf.* 18 U.S.C. § 2510(14) (encrypted radio communications are not readily accessible to the public). Just as a locked door creates an expectation of privacy, *see United States v. Carriger*, 41 F.2d 545 (8th Cir. 1976), the steps that KaZaA took to protect electronic communications on the KaZaA network make tapping into those communications without authorization an example of criminal wiretapping.

The Internet is an electronic communications system. At the level of TCP/IP packet communications (as opposed to at the level of web browsers that translate such communications into human-readable form), the Internet is not readily accessible to the general public. *See Konop v. Hawaiian Arilines, Inc.*, 236 F.3d 1035 (9th Cir. 2001) (Internet should be treated analogously to other communication networks: "We believe that Congress intended the ECPA to eliminate distinctions between protection of private

communications based on arbitrary features of the technology used for transmission."); Douglas C. Sicker, Paul Ohm, Dirk Grunwald, *Legal Issues Surrounding Monitoring During Network Research*, Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement 141–48 (October 24–26, 2007) (discussing legal issues involved with packet sniffers and failing to identify § 2511(2)(g)(i) as a legal exception that would exempt packet sniffing).

The communications system at the TCP/IP level requires special expertise to access. *See, e.g.,* Craig Hunt, TCP/IP Network Administration (2d Ed. 1998); Mark S. Burgess, Principles of Network and System Administration (2000). This is why the RIAA and its lawyers engaged MediaSentry in the first place: they needed to break into the Internet at this level (rather than at the publicly accessible level of web browsers and the like) in order to decrypt the TCP/IP packets flowing between MediaSentry's computer and Joel's. An ordinary person could not have done this because the Internet is not designed for ordinary people to listen in on such packet transmissions. And it is no defense to say that MediaSentry merely recorded data (TCP/IP packets) sent to it. Packets on arrival but before conversion to human-readable form are protected and may not be tapped, just like a tap in the receiver of a phone is no less objectionable than a tap on the main line. *See United States v. Councilman*, 418 F.3d 67, 79 (1st Cir. 2005).

If this Court holds otherwise, the Internet will have no protection under the wiretap laws: any party could intercept TCP/IP packets — the packets that transmit all data over the Internet — without regard for legal consequences. To see only one absurd consequence of this rule, consider voice over IP (VOIP), the technology used for Internet telephone calls on systems like Skype or Vonage. If Plaintiffs are right, then ordinary

phone calls would be protected, but VOIP calls would not. Ordinary mail would be protected, but email would not. "It makes no more sense that a private message expressed in a digitized voice recording stored in a voice mailbox should be protected from interception, but the same words expressed in an e-mail stored in an electronic post office pending delivery should not." *Konop*, 236 F.3d at 1046. This was not what Congress intended when it added "electronic communications" to the Wiretap Act in 1986.

The Supreme Court has observed that the Wiretap Act has as its dual purpose (1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized. *Gelbard v. United States*, 408 U.S. 41, 48 (1972) (citing S. Rep. No. 1097, 90th Cong., 2d Sess., 66 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153). The Court also noted that: "[a]lthough Title III authorizes invasions of individual privacy under certain circumstances, the protection of privacy was an overriding congressional concern." *Id.* In 1986, Congress amended Title III to include electronic communications, with the idea in mind that the wiretap laws had to be updated in order to take into account new telecommunication technologies. *See United States v. Herring*, 933 F.2d 932, 935 (11th Cir.1991).

Because no exceptions to the Wiretap Act's prohibition on interception of electronic communications apply, the interception that MediaSentry used to gather the evidence now deployed against Joel Tenenbaum in this case constituted a criminal violation of the Wiretap Act. *See* 18 U.S.C. § 2511(4)(a).

**D. Massachusetts Wiretap Statute**

MediaSentry also violated the Massachusetts Wiretap Statute. The preamble to that statute explains that its purpose is to prohibit electronic surveillance by private individuals:

> The general court further finds that the uncontrolled development and **unrestricted use of modern electronic surveillance devices pose grave dangers to the privacy of all citizens** of the commonwealth. **Therefore, the secret use of such devices by private individuals must be prohibited.** The use of such devices by law enforcement officials must be conducted under strict judicial supervision and should be limited to the investigation of organized crime.

M.G.L. 272 § 99(A) (emphasis added). Just like the federal statute, the Massachusetts statute prohibits interception of communications. M.G.L. 272 § 99(C) (prohibiting interception and providing for punishment of up to five years' imprisonment). And unlike the federal statute, the Massachusetts statute requires both parties' consent, not merely one party's consent, before recording is exempted fro the statute. *See* M.G.L. 272 § 99(B)(4) (defining *interception*). The Rhode Island wiretapping statute parallels the federal statute. *See* R.I. Stat. § 12-5.1-1 *et seq.*

## II. THIS COURT CAN AND, IN THE INTEREST OF JUSTICE AND DETERRENCE, SHOULD SUPPRESS THE ILLEGALLY OBTAINED EVIDENCE AGAINST JOEL TENENBAUM

All federal courts have the power to control proceedings in the interest of ensuring that federal process is just. This power, which has been described as the "inherent power," derives from Article III of the Constitution:

> I agree with the Court that Article III courts, as an independent and coequal Branch of Government, derive from the Constitution itself, once they have been created and their jurisdiction established, the authority to do what courts have traditionally done in order to accomplish their assigned tasks. Some elements of that inherent authority are so essential to "the Judicial Power," U.S. Const. art. III § 1, that they are indefeasible, among which is a court's ability to enter orders protecting the integrity of its proceedings.

*Chambers v. NASCO, Inc.*, 501 U.S. 32, 58 (1991) (Scalia, J., dissenting); *see also id.* at 46–51 (majority opinion). The inherent power prevents the unmanning of a court in the face of conduct that challenges the integrity of federal process.

A court may remedy abuse of process through its inherent power by imposing remedies up to and including dismissal of a case. *See id.* at 44 ("A primary aspect of that discretion is the ability to fashion an appropriate sanction for conduct which abuses the judicial process. As we recognized in *Roadway Express*, outright dismissal of a lawsuit, which we upheld in *Link*, is a particularly severe sanction, yet is within the court's discretion."); *United States v. Smiley*, 553 F.3d 1137, 1142 (8th Cir. 2009) (recognizing district court's inherent power and citing *Chambers*); *Lamb Engineering & Construction Co. v. Nebraska Public Power District*, 103 F.3d 1422, 1434–37 (8th Cir. 1997) (same).

District courts have often used their inherent power to suppress evidence obtained in violation of the ethical rules governing lawyers. The United States District Court for the District of Delaware, for example, suppressed all evidence collected by Fish & Richardson's questioning of an employee of a defendant in a patent-infringement case where they knew that the defendant was represented by counsel. Judge Robinson explained:

> [T]he violation of the Model Rules must be recognized and deterrence enforced through the imposition of a sanction. Therefore, . . . plaintiff may not use the fruits of F & R's conduct, that is, plaintiff's expert, Mr. Chang, may not serve as a consultant or expert witness in this litigation, nor may the two F & R lawyers who oversaw the installation be involved in the litigation, nor may the information be given to any other witness for use in this litigation.

*Microsoft Corp. v. Alcatel Business Systems*, No. 07-090-SLR, 2007 WL 4480632 at *1–*2 (D. Del. 2007). Because the inherent power stems directly from the Constitution, exercising it to suppress evidence is consistent with Rule 402. *Cf. Bell Atlantic Corp. v.*

*Bolger*, 2 F.3d 1304, 1316 (3d Cir. 1993) ("The ethical standards imposed upon attorneys in federal court are a matter of federal law.").

Similarly, when Dickie Scruggs paid $150,000 per year to material witnesses in the Katrina insurance litigation in violation of the ethical rule forbidding investigation by this means, the United States District Court for the Southern District of Mississippi suppressed the evidence that he had collected by this means. *See McIntosh v. State Farm Fire & Casualty Co.*, No. 1:06C-cv-1080-LTS-RHW, 2008 WL 941640 at *3 (S.D. Miss. 2008). Judge Senter expressly rested his decision to exclude their testimony on Scruggs's having violated the ethical rule regarding payment of material witnesses, even citing a Mississippi State Bar Ethics Committee opinion on point. *See id.* at *2. *See also Hammond v. City of Junction City*, 167 F. Supp. 2d 1271, 1293 (D. Kan. 2001) (suppressing unethically obtained evidence); *Cagguila v. Wyeth Labs, Inc.*, 127 F.R.D. 653, 654–55 (E.D. Pa. 1989) (same); *Aiken v. Business and Industry Health Group, Inc.*, 885 F. Supp. 1474, 1480 n.7 (D. Kan. 1995) ("Strict adherence to these rules is demanded and any information gained in violation of an applicable ethical guideline remains subject to suppression.").

The First, Third, and Seventh Circuits have expressly recognized district courts' discretion to suppress unethically obtained evidence. *See United States v. Miller*, 624 F.2d 1198, 1201 (3d Cir. 1980) ("The district court [has] inherent authority to supervise the professional conduct of attorneys appearing before it. As a general rule, the exercise of this authority is committed to the sound discretion of the district court."); *Trans-Cold Express, Inc. v. Arrow Motor Transit, Inc.*, 440 F.2d 1216, 1219 (7th Cir. 1971) ("the desirability of deterring improper investigative conduct was a factor which the court

could properly consider in the exercise of its discretion to exclude the evidence"); *Borges v. Our Lady of the Sea Corp.*, 935 F.2d 436, 440 (1st Cir. 1991) ("Insofar as Orlando appears to have acted improperly in obtaining the statement as counsel for Borges, such impropriety in the means of obtaining a statement would not automatically bar admission of the statement at trial. There is no exclusionary rule in civil cases. If the issue were raised, the decision whether to exclude the evidence would be in the district court's discretion.").

"The ethical standards imposed upon attorneys in federal court are a matter of federal law. We look to the Model Rules of Professional Conduct to furnish the appropriate ethical standard." *Bell Atlantic Corp. v. Bolger*, 2 F.3d 1304, 1316 (3d Cir. 1993). The Model Rules of Professional Conduct, like the Massachusetts Rules of Professional Conduct, forbid "methods of obtaining evidence that violate the legal rights of . . . a [third] person." Rule 4.4. The methods of obtaining evidence employed by MediaSentry violated the legal rights of Joel Tenenbaum under the Private Detectives Act, the Wiretap Act, and the Massachusetts Wiretap Statute as described in Part I, *supra*. *Cf.* ABA Formal Opinion 01-422: Electronic Recordings by Lawyers (holding, in the context of voice recordings, that violation of state wiretap laws is violation of rules of professional conduct). In all respects relevant to this case, the Massachusetts Rules of Professional Conduct, the Colorado Rules of Professional Conduct, the Rhode Island Rules of Professional Conduct, and the ethical rules of most other states mirror the Model Rules.

The Model Rules make lawyers responsible for misconduct by persons whom they are supervising when the lawyer approves the conduct or learns of the conduct in time to avoid or mitigate its consequences:

> With respect to a nonlawyer employed or retained by or associated with a lawyer: . . .
>
> (c) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:
>
> > (1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or
> >
> > (2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

Rule 5.3.

The lawyers who orchestrated the RIAA's litigation campaign were ethically responsible for the conduct of MediaSentry, their "investigative arm." These lawyers knew or should have known that MediaSentry's activities were illegal at latest when MediaSentry began receiving notice from states that its actions were in violation of state private detective and wiretapping. Moreover, these lawyers were intimately involved in crafting MediaSentry's investigative strategy and reviewing the dossiers that MediaSentry brought in.

In a declaration filed in *UMG Recordings Inc. v. Lindor*, No. 05-cv-1095 in the United States District Court for the Eastern District of New York, Bradley A. Buckles, the RIAA's Executive Vice President, Anti-Piracy, explained the close relationship between the RIAA's lawyers and MediaSentry. Buckles declared:

> [T]he MediaSentry Agreement provides detailed information regarding the instructions and parameters for conducting on-line investigations that were discussed and developed by the RIAA and its counsel, on behalf of the RIAA's members. . . .
>
> As the detailed instructions and search parameters of the MediaSentry Agreement show, MediaSentry was intimately involved in the formulation of the legal strategy developed by the RIAA's anti-piracy team, including the record companies' counsel. This strategy formed the basis of the legal advice that was provided to the record companies regarding how best to investigate and capture infringers, and this legal advice, which I believe to be subject to the attorney-client privilege, is reflected in the MediaSentry Agreement. Moreover, the information contained in the MediaSentry Agreement and the Agreement itself were generated directly and exclusively because of potential litigation, and these documents reflect the mental impressions of counsel, particularly as to the record companies' and their counsel's strategy for enforcing the record companies' substantial copyright interests.

According to Buckles, MediaSentry was so deeply integrated with the RIAA's legal team that the privilege extends to the RIAA's engagement agreement with MediaSentry.

As a matter of federal substantive law, this Court has the inherent power to suppress evidence obtained in violation of the ethics rules that apply in federal court. *See Aiken*, 885 F. Supp. at 1480 n.7; *see also State v. Ford*, 539 N.W.2d 214 (Minn. 1995) (supervisory power includes power to suppress evidence); *O'Brien v. O'Brien*, 899 So. 2d 1133, 1137–38 (Fla. App. 2005) (suppressing evidence obtained in violation of the Wiretap Act and collecting cases on discretion of trial courts to suppress evidence).

## III. CONCLUSION

This motion raises a question of fairness. May the recording industry rest its entire campaign on evidence collected by dubious means when that campaign is being waged against individuals with neither the resources nor the wherewithal to question the manner in which this evidence is being collected? In this, one of the few cases being vigorously contested, we pray this Court will answer no.

Respectfully submitted,

/s/ Charles R. Nesson
Charles R. Nesson
1575 Massachusetts Avenue
Cambridge, MA 02138
617-495-4609
nesson@law.harvard.edu

/s/ K.A.D. Camara
K.A.D. Camara*
Camara & Sibley LLP
2339 University Boulevard
Houston, Texas 77005
713 893 7973
713-583-1131 (fax)
camara@camarasibley.com

*Attorneys for Defendant Joel Tenenbaum*

Dated: June 23, 2009

* Mr. Camara is a member of the Massachusetts Bar (BBO# 661087) and of the Texas Bar. He will promptly apply for admission to the bar of this Court or move this Court for permission to appear *pro hac vice* in this matter.

**CERTIFICATE OF SERVICE**

I hereby certify that on June 23, 2009, I served the foregoing document on counsel of record by CM/ECF as follows:

Eve Burton
Holme, Roberts & Owen LLP
1700 Lincoln, Suite 4100
Denver, Colorado 80203

/s/ Charles R. Nesson
Charles R. Nesson