UNITED STATES DISTRICT COURT

DISTRICT OF MASSACHUSETTS

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

PLAINTIFFS' OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS EVIDENCE

Plaintiffs submit this response in opposition to Defendant's Motion to Suppress Evidence (Doc. No. 853),[1] and state as follows:

INTRODUCTION

Defendant's Motion to Suppress is premised on an entirely fictional set of facts and law. Factually, Defendant's Motion fundamentally misconstrues how information travels on the Internet, how KaZaA and the FastTrack network operate, and the actions taken by MediaSentry to record copies of the files and data sent to it. All of the information collected by MediaSentry was available to any user of the FastTrack network – millions of users at any given time. All MediaSentry did was record or document the information that was sent by Defendant to

[1] Consistent with Defendant's practice throughout this case, Defendant has again failed to confer in good faith with Plaintiffs under Local Rule 7.1(a)(2) before filing this motion.

MediaSentry. The recording by a recipient of information sent to that recipient cannot be, and was not, a violation of the law and, as such, it should not be suppressed. None of the statutes Defendant claims MediaSentry to have violated provide for the exclusion of evidence. In short, MediaSentry did not violate any State or Federal law and there is no basis for excluding evidence gathered by MediaSentry.

Legally, it is hornbook law that the Fourth Amendment, and thus the exclusionary rule, does not apply in civil cases. As this Court recently explained, in rejecting a similar motion, filed by a Doe Defendant in part of the consolidated cases brought by the record companies, regarding virtually identical evidence by MediaSentry, "[n]either the rules of evidence nor the Fourth Amendment bar the use of evidence arguably unlawfully obtained by private parties in their private suits." *London-Sire Records, Inc. v. Doe 1*, Case No. 07CV10834-NG, slip op. at 3-4 (D. Mass. Jan. 9, 2009) (Gertner, J.) (attached hereto as Exhibit A). In that case, the Court considered an argument almost identical to the one at bar which sought to exclude the very type of evidence gathered by MediaSentry that Defendant challenges in his Motion to Suppress here. This Court concluded that "[e]ven assuming [defendant] is correct that MediaSentry's evidence was illegally obtained, that is not enough to strike it." *Id.* The same principle applies in this case, and the Court should deny Defendant's Motion.

Defendant's unsupported and unsubstantiated (and unprofessional) attacks on Plaintiffs (and their counsel) are simply unfounded. As numerous courts around the country have held, in considering similar claims made by other defendants in similar file-sharing cases, Plaintiffs actions in detecting and pursuing claims of copyright infringement were neither unethical nor illegal. Plaintiffs were simply protecting their rights and their intellectual property. As the Court

explained in a similar file-sharing case, *Atlantic Recording Corp. v. Heslep*, 2007 U.S. Dist. LEXIS 35824, at *16 (N.D. Tex. 2007):

> The Court rejects [the defendant's] characterization of this lawsuit, and many others like it, as "predatory." Plaintiffs' attorneys brought this lawsuit not for the purposes of harassment or to extort [] as she contends, but, rather to protect their clients' copyrights from infringement and to help their clients deter future infringement. The evidence uncovered from MediaSentry's investigation shows that Plaintiffs' allegation of [] alleged copyright infringement have evidentiary support and will likely have more evidentiary support through further investigation and discovery. For now, our government has chosen to leave the enforcement of copyrights, for the most part, in the hands of the copyright holder. Plaintiffs face a formidable task in trying to police the internet in an effort to reduce or put a stop to the online piracy of their copyrights. Taking aggressive action, as Plaintiffs have, to defend their copyrights is certainly not sanctionable conduct under Rule 11. The right to come to court to protect one's property rights has been recognized in this country since its birth.

Id. at *16. *See also* June 15, 2009 Order (Doc. Text Order, These lawsuits do "not amount to an abuse of process"). It cannot be a violation of either the ethics rules or the law for a copyright owner to log on to a peer-to-peer network, as any other user of the network could do, request their copyrighted files which are being distributed to other users on the network, and then record the information sent to it. Indeed, Defendant has not – and cannot – cite a single authority that holds this conduct to be violative of laws or ethics.

Finally, the District of Minnesota recently rejected an identical motion asserted by the same counsel in *Capitol Records, Inc. v. Thomas-Rasset*, Case No. 06-cv-1497-MJD-RLE (D. Minn.). In the *Thomas-Rasset* case, the court found that counsel's arguments had no merit and denied it. *See Capitol Records, Inc. v. Thomas-Rasset*, Case No. 06-cv-1497-MJD-RLE, slip op. at 2-12 (D. Minn. June 11, 2009) (denying defendant's motion to suppress evidence by MediaSentry because defendant failed to show MediaSentry violated any law in gathering evidence to be used in the case) (hereinafter *Thomas-Rasset*, attached hereto as Exhibit B). Specifically, the *Thomas-Rasset* court held that:

> MediaSentry did not illegally obtain the evidence in question. MediaSentry acted for the legitimate purpose of discovery infringers and protecting its clients' copyrights. Therefore, there was no ethical violation committed by Plaintiffs' attorney' involvement with MediaSentry's investigation. . . . Because Defendant has failed to show that MediaSentry violated any law in gathering the evidence to be used in this case, Defendant's motion to suppress is denied.

Id. For all of these reasons and those explained below and in the *Thomas-Rasset* decision, Defendant's Motion to Suppress should be denied.

BACKGROUND

Peer-to-peer networks allow people to connect to each other to distribute files, including, in large measure, audio files containing popular copyrighted music. Unlike the World Wide Web (web sites) where data is stored on central web services and users connect to a central web server to download information from the web site, peer-to-peer networks allow users to connect to each other and transfer files directly from user to user. (Declaration of Doug Jacobson ("Jacobson Decl.") at ¶ 2, attached hereto as Exhibit C.)

When files are distributed from one user to another on the KaZaA peer-to-peer network, a set of identifiers tie the files back to the user distributing the files. These include (a) the IP address of the client distributing the files, (b) the name of the file, (c) file size, (d) the content hash, and (e) the port information. (*Id.* at ¶ 3.) At no time during the process of communicating or sharing files does one user gain entry into another user's computer. (*Id*. at ¶ 5.) Rather, the user requesting files simply communicates a request that the sharing computer send files, and the sharing computer sends the files. (*Id*.) Neither KaZaA, nor any other popular file-sharing program, permits one user to gain access into or in any way alter or manipulate the contents of another user's computer, or even to view any contents of another user's computer except those placed in a shared folder. (*Id*.)

In this case, MediaSentry did not need to take any kind of extraordinary steps in order to document the IP address of the computer from which it downloaded music files. (*Id*. at ¶ 6.) The IP address is transmitted as part of the normal process of connecting one computer to another over the Internet. (*Id*.) When identifying infringers on peer-to-peer networks, MediaSentry does only what any other user on the network can do. (Declaration of Chris Connelly ("Connelly Decl.") at ¶ 2, attached hereto as Exhibit D.) It uses the same network protocols used by every other user on the network to search for and download files. (*Id*.) Files transferred from the uploader's computer to MediaSentry are sent by the uploader in the form of data packets, which contain information identifying the source IP address, *i.e.*, the IP address for the computer from which the file is being transferred. (*Id*.) Using widely used packet capture technology, MediaSentry records the interaction between itself and a computer connected to the file sharing network at a specific IP address in order to show the file and data transfer from that computer. (*Id*.)[2] In other words, when downloading files from another user on a peer-to-peer network, the downloading process itself allows MediaSentry to identify the computer distributing the copyrighted material from a specific IP address. (*Id*.) MediaSentry captures this IP address information, along with other information about the file, including the specific date and time of file transfer. (*Id*.)

As numerous courts around the country have held, the information available on peer-to-peer networks is public information, readily accessible to anyone who wants it, and for which there is no reasonable expectation of privacy. As Judge Davis recently explained in response to the virtually identical motion in *Thomas-Rasset*:

[2] Indeed, this packet capture technology is so ubiquotous that it is widely available for use on most major operating systems, including Windows. (Jacobson Decl. at ¶ 8.)

> ***There is no expectation of solitude or seclusion when a person activates a file sharing program and sends a file to the requesting computer***. By participating in Kazaa, a user expects millions of other users to view and copy her files, each time receiving the very information that [Defendant] sent to MediaSentry and MediaSentry recorded.

Thomas-Rasset, slip op. at 11-12 (Ex. B) (emphasis added); *see also In re Verizon Internet Servs., Inc.*, 257 F. Supp. 2d 244, 267 (D.D.C. 2003) (holding that when an ISP subscriber "opens his computer to permit others, through peer-to-peer file sharing, to download materials from that computer, it is hard to understand just what privacy expectation he or she has after ***essentially opening the computer to the world***.") (emphasis added), *rev'd on other grounds*, 351 F.3d 1229 (D.C. Cir. 2003); *Elektra Entm't Group, Inc. v. Does 1-9*, 2004 WL 2095581, at *5 (S.D.N.Y. Sep. 8, 2004) (holding Defendant has "minimal 'expectation of privacy in downloading and distributing copyrighted songs without permission'"); *United States v. Kennedy*, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (activation of file-sharing mechanism shows no expectation of privacy); *Sony Music Entertainment Inc. v. Does 1-40*, 326 F. Supp. 2d 556, 566 (S.D.N.Y. 2004) ("defendants have little expectation of privacy in downloading and distributing copyrighted songs without permission"); *Arista Records, L.L.C. v. Tschirhart*, Case No. 05-CV-372-OLG, slip op. at 6 (W.D. Tex. May 24, 2006) (attached hereto as Exhibit E) ("[a] user of a P2P file-sharing network has little or no expectation of privacy in the files he or she offers to others for downloading"). This is especially true in this case where Defendant testified that he was specifically aware of people downloading files from his computer over KaZaA. (Deposition of Joel Tenenbaum dated September 24, 2008 157:4-158:3, relevant excerpt attached hereto as Exhibit F.)

ARGUMENT

Defendant seeks to suppress evidence gathered by MediaSentry arguing that MediaSentry violated (1) the Massachusetts Private Detectives Act (the "MPDA"), (2) the Electronic Communications Privacy Act of 1986 (the "Federal Wiretap Act"), and (3) the Massachusetts Wiretapping Statute.[3] As demonstrated below, not only is Defendant wrong on the facts, but he is wrong on the law as well.

I. This Court Already Rejected The Argument That MediaSentry's Evidence Should Be Excluded Based On Violations Of The MPDA And The Wiretap Act.

In *London-Sire Records, Inc. v. Doe 1*, this Court rejected a similar motion regarding virtually identical evidence from MediaSentry and held that "[n]either the rules of evidence nor the Fourth Amendment bar the use of evidence arguably unlawfully obtained by private parties in their private suits." *See* slip op. at 3-4. The Court concluded, that "[e]ven assuming [defendant] is correct that MediaSentry's evidence was illegally obtained, that is not enough to strike it." *Id.* As this Court has already decided this very issue, Defendant's Motion here should be summarily denied.

II. MediaSentry Did Not Violate The MPDA.

A. The MPDA has no application to MediaSentry or its activities in this case.

Defendant's contention that MediaSentry violated the MPDA fails for several reasons. First, Defendant has stated that his computer which was connected to his Internet account with Cox Communications, Inc. on August 10, 2004 was *located in Rhode Island*, not in

[3] Plaintiffs note the irony in Defendant's counsel complaining of a violation of the Massachusetts Wiretap Statute, as the Court has previously criticized Defendant's counsel for his conduct which has violated this law. (Order, Doc. No. 850.)

Massachusetts.[4] (*See* Subpoena to Cox Communications, Inc. dated November 3, 2004 ("Cox Subpoena"), attached hereto as Exhibit G, and Subpoena Response from Cox Communications, Inc. ("Cox Subpoena Response"), attached hereto as Exhibit H.) As such, Defendant's argument that MediaSentry violated a Massachusetts licensing scheme has no factual basis whatsoever because neither Defendant nor MediaSentry were located in Massachusetts at the time of the conduct in question.

Second, Defendant has not provided any authority to support the idea that MediaSentry is even subject to the MPDA. Nor could he. The MPDA does not apply to persons or companies operating outside of the Commonwealth of Massachusetts. *See* ALM GL ch. 1, § 2 (2009) (providing that jurisdiction of the commonwealth "shall extend to all places within its boundaries"). Massachusetts' licensing scheme cannot apply to non-Massachusetts entities conducting activities in other states, especially where such entities may be subject to other licensing requirements. *See Healy v. Beer Inst.*, 491 U.S. 324, 36 (1989) (a statute that seeks to control commerce occurring wholly outside the boundaries of a state "exceeds the inherent limits of the enacting State's authority and is invalid."). Here, MediaSentry does not operate in the Commonwealth of Massachusetts and conducted no investigation within Massachusetts that could possibly subject it to the Commonwealth's licensure requirements.[5] (Connelly Decl. ¶ 3.) MediaSentry has no employees in the Commonwealth of Massachusetts and does not conduct

[4] To the extent Defendant claims MediaSentry violated the Rhode Island Private Detective Act, R.I. Gen. Laws § 5-5-1 *et seq.*, as with the MDPA and for the same reasons, it does not apply. Additionally, § 5-5-21 of the statute provides the available remedies, which does not include exclusion of evidence.

[5] Defendant's contention that MediaSentry could not have satisfied the requirements for licensure in Massachusetts (Def's Motion at 6) proves Plaintiffs' point that Massachusetts' licensing scheme is not designed to cover entities such as MediaSentry that operate beyond the boundaries of the Commonwealth. MediaSentry never intended to reside in a community within the Commonwealth, thus removing MediaSentry from the ambit of ALM GL ch. 146, § 24.

any activities in the Commonwealth. (*Id.*) It does not pay taxes in Massachusetts and does not have an agent for service of process in the Commonwealth. (*Id.*) Most significantly, MediaSentry conducted no activity whatsoever in the Commonwealth of Massachusetts relating to this case. (*Id.*) All of the information MediaSentry received was sent by Defendant from his computer located in Rhode Island to MediaSentry's computer in another state. (*Id.*; Cox Subpoena and Cox Subpoena Response, Exs. G, H.)

Moreover, the MPDA regulates persons operating in quasi-police roles – applicants typically must have been regularly employed for at least three years doing investigative work which can include a United States investigative service or a former police officer of a rank or grade higher than that of patrolman. *See* ALM GL ch. 147, § 24 (2009). As explained above, the type of work performed by MediaSentry, the gathering of public information that was placed on the Internet, does not come close to playing a quasi-police role and certainly does not implicate the MPDA. There was no private investigation here because the information that MediaSentry gathered is public information sent to MediaSentry by Defendant's computer, over a peer-to-peer network. (Connelly Decl. at ¶ 2; *see also* Jacobson Decl. at ¶ 6.). As Judge Davis explained in rejected a virtually identical motion in *Thomas-Rasset*, "Merely monitoring incoming internet traffic sent from a computer in another state is insufficient to constitute engaging in the business of private detective within the state of Minnesota." *Thomas-Rasset,* slip op. at 6-7 (Ex. B). The same holds true in this case.

Third, Defendant has not cited any authority indicating that he has standing to assert claims under the MPDA. The MPDA contains no provision authorizing a private party to enforce the statute. Rather, the MPDA places exclusive enforcement authority in the Commissioner of Public Safety. *See* ALM GL ch. 147, § 1 (2009) (charging the commissioner

of public safety with "the administration and enforcement of all laws, rules and regulations"). Thus, Defendant lacks standing to enforce the MPDA. Because Defendant lacks standing to bring claims under the MPDA, the Court does not have jurisdiction to hear her argument. *See CytoLogix Corp. v. Ventana Med. Sys.*, 2007 U.S. Dist. LEXIS 77065, at *5-6 (D. Mass. Oct. 17, 2007) (if a plaintiff lacks standing, the district court has no subject matter jurisdiction over a claim).

Finally, it should be noted that the factual basis for Defendant's argument is incomplete and does not help him. As provided as Exhibit A to Defendant's Motion to Suppress, MediaSentry received a letter, dated January 2, 2008, from a Sergeant Bishop in the Certification Unit of the Department of State Police, indicating that MediaSentry did not appear to have a private investigators license under the MGL Provisions. By letter dated January 10, 2008, counsel for MediaSentry disputed Sergeant Bishop's initial assessment. Since then, MediaSentry has received no further communication from the State Police. There has never been any investigation or finding that MediaSentry was subject to, let alone violated, the MDPA.

B. The MPDA provides no basis for excluding any evidence in this case.

Not only has there been no violation of the MPDA, the MPDA provides no basis for excluding evidence. No provision of the MPDA supports the exclusionary rule as a remedy for alleged violations of the MPDA and no court has interpreted a violation of the MPDA to invoke the exclusionary rule. In fact, when discussing the penalty for violating the Commonwealth's license requirements, there is no mention of exclusion of evidence. *See* ALM GL, ch. 146 § 23 (2009).

Indeed, the Federal District Court for the District of Maine, when interpreting a similar licensing statute, held that that failure of a witness to obtain a private investigator's license did

not warrant excluding his testimony at trial. In *TNT Road Co. v. Sterling Truck Corp.*, 2004 U.S. Dist. LEXIS 13463, at *6 (D. Me. July 19, 2004), the Court concluded that:

> Assuming that [the expert] was required by Maine law to have a license to conduct his investigation of the vehicle fire in this case, I am not persuaded that his failure to do so justifies the exclusion of his testimony. Nor do I think that his failure to obtain a license prevents the court from considering his expert qualifications or the reliability of his investigatory methods.

Id at * 6; *see also, London-Sire Records, Inc. v. Doe 1*, slip op. at 3-4 ("[e]ven assuming [defendant] is correct that MediaSentry's evidence was illegally obtained, that is not enough to strike it.")

For these reasons, the MPDA has no application here and provides no basis for excluding evidence.

III. MediaSentry Did Not Violate The Federal Wiretap Act And The Act Does Not Provide For Exclusion Of Evidence.

A. MediaSentry's actions did not violate the Federal Wiretap Act.

The Federal Wiretap Act prohibits the *interception* of any wire, oral or electronic communication, without consent. 18 U.S.C. § 2511 *et seq*. It does not prohibit the interception of a communication when "one of the parties . . . has given prior consent . . . ." 18 U.S.C. § 2511(2)(d).

Here, Defendant consented to MediaSentry's download by placing the copyrighted sound recordings in a share folder accessible to the general public where they would be distributed to other users on the network. *See Thomas-Rasset*, slip op. at 11-12 (Ex. B, "There is no expectation of solitude or seclusion when a person activates a file sharing program and sends a file to the requesting computer. By participating in Kazaa, a user expects millions of other users to view and copy her files, each time receiving the very information that [Defendant] sent to MediaSentry and MediaSentry recorded."); *In re Verizon Internet Servs.*, 257 F. Supp. 2d at 267

(When an ISP subscriber "opens his computer to permit others, through P2P file sharing, to download materials from that computer, it is hard to understand just what privacy expectation he or she has after essentially opening the computer to the world."). In so doing, Defendant is not protected by the Federal Wiretap Act.

Additionally, not only did Defendant consent, but the communication at issue occurred between Defendant and MediaSentry, and there can be no dispute that MediaSentry consented to its documentation of the information sent to it from Defendant's computer.

Defendant argues that the consent exception (18 U.S.C. §2511(2)(d)) does not apply because the communication was "intercepted for the purpose of committing any crime or tortious act." This argument is absurd and was summarily rejected by *Thomas-Rasset* court:

> MediaSentry was clearly a party to the electronic communication with Defendant. . . . MediaSentry did not intercept the communications for the purpose of committing a crime or tort. . . . Even if, in capturing the information sent from Defendant's computer, MediaSentry had incidentally violated a private detective licensing statute from another state, gathering evidence of Defendant's alleged copyright infringement cannot be said to have been accomplished for the purpose of committing a crime or tort.

Thomas-Rasset, slip op. at 10-11 (Ex. B) (emphasis in original); *see also Columbia Pictures Indus. v. Bunnell*, 2007 U.S. Dist. LEXIS 46364, at *41 (C.D. Cal. May 29, 2007) ("As defendants' website is the intended recipient of the Server Log Data, and defendants can lawfully intercept and consent to the disclosure thereof, this statutory provision, even if applicable would not provide a basis to withhold such data which is clearly within defendants' possession, custody and control.").

In short, Plaintiffs gathered the MediaSentry information to protect their copyrights from rampant infringement on the Internet. *See, e.g.*, *Heslep*, 2007 U.S. Dist. LEXIS 35824, at *16. Defendant offers no support for his contention that the communication was intercepted *for the purpose of* committing a crime or tort, and such an allegation is factually spurious. It makes no

sense that MediaSentry would obtain information regarding Defendant's copyright infringement over a peer-to-peer network *for the purpose* of violating the MPDA or the MWS. *See Thomas-Rasset*, slip op. at 10-11 (Ex. B). And while Defendant and his counsel may disagree with Plaintiffs' decision to litigate cases like this one, there can be no question that gathering the evidence of Defendant's copyright infringement cannot be reasonably said to have been "for the purpose of committing" a crime or tort. *Id*. Indeed, the evidence was obtained by MediaSentry in order to stop others from committing in improper behavior. Section 2511(2)(d)'s exception applies and MediaSentry's recording of the evidence of Defendant's copyright infringement does not fall within the confines of the Federal Wiretap Act.

Further, the Federal Wiretap Act states that it shall not be unlawful to "access an electronic communication made through a [computer] that is configured so that such electronic communication is readily accessible to the general public." 18 U.S.C. §2511(2)(g)(i). This exception to protected communications specifically excludes Defendant from protection because he placed the sound recordings in a shared folder designed to be accessed by the general public. *See Thomas-Rasset*, slip op. at 11-12 (Ex. B). Defendant's argument that KaZaA is not open to the public is simply wrong. KaZaA and the FastTrack network at issue allow millions of users to trade files. Moreover, KaZaA is free and available to anyone who wants it and requires only basic registration information. (Jacobson Decl. at ¶ 7.) Obtaining and installing KaZaA can be done anonymously and easily by anyone with an Internet connection. (*Id*.) Moreover, contrary to Defendant's unsupported assertion, KaZaA does not require a password. (*Id*.) There is no question that KaZaA is open and readily accessible to the general public.[6] The fact that the

[6] Defendant's argument that the KaZaA terms of use show that KaZaA was not generally accessible to the public is both incorrect and a red herring. It would be ironic indeed if the terms of use of KaZaA could somehow immunize copyright infringers and prevent copyright

(continued…)

mechanical process requires downloading the software does not make it non-public because the software is available to anyone on the Internet.

Moreover, the Federal Wiretap Act is not implicated in this case because, as to electronic communications, it only prohibits ***interception*** during transmission (not while in electronic storage, i.e., RAM), and the disclosure of electronic communications intercepted during transmission. *Konop v. Hawaiian Airlines, Inc*., 302 F.3d 868, 878-79 (9th Cir. 2002). Here, MediaSentry did not *intercept* the electronic communication during transmission but merely recorded and retained the electronic communication after it was sent directly to it.[7]

B. The Federal Wiretap Act does not provide for exclusion of evidence.

The exclusionary provision of 18 U.S.C. § 2515 applies to "wire and oral communication[s]" but not to "electronic communications" as defined in the Act. *See United States v. Steiger*, 318 F.3d 1039, 1050 (11th Cir. 2003) ("By its terms, 18 U.S.C.S. § 2515 applies only to wire communications, and not to electronic communications.") A "wire or oral communication" under the Federal Wiretap Act typically involves an actual aural communication between persons. *See Lanier v. Bryant*, 332 F.3d 999, 1002 (6th Cir. 2003) (involving intercepted telephone conversations). Since the communication at issue here was

---

(…continued)
holders from protecting their copyrights. Defendant has no right to enforce the clearly invalid KaZaA terms of use. To the extent the KaZaA terms of use suggest that a copyright holder cannot enforce its rights, they are ultra vires and without effect. Defendant cannot hide behind the KaZaA terms of use to shield his illegal activity.

[7] Defendant's argument that rejecting Defendant's argument would result in no protection for Internet communications is simply incorrect. It would still protect communications truly intercepted without the consent of a party to the communication. As Judge Davis explained in *Thomas-Rasset*, the Wiretap Act's one party consent exception was aimed at "monitoring . . . for insidious purposes" and the exception applied when the recorder's "purpose is evil." *Thomas-Rasset*, slip op. at 11 (Ex. B).

electronic, the statute itself rejects exclusion, even in criminal cases. Additionally, the exclusionary provision of 18 U.S.C. § 2515 was not meant to apply in a civil proceeding. *See Philadelphia Resistance v. Mitchell*, 58 F.R.D. 139, 147 (E.D. Pa. 1972) ("Congress only intended to limit discovery in the context of criminal and not civil proceedings.")

IV. MediaSentry Did Not Violate The Massachusetts Wiretap Statute And The Statute Does Not Provide For The Exclusion Of Evidence In A Civil Case.

A. MediaSentry's actions did not violate the Massachusetts Wiretap Statute.

Defendant's contention that MediaSentry violated the Massachusetts Wiretap Statute fails for several reasons. First, the irony of this argument is clear, as this Court has held, on several occasions, that Defendant's counsel has repeatedly violated this very statute. (Order Re: Motion to Stay, Feb. 12, 2009, Doc. No. 759, at 4; Order, Jun. 16, 2009, Doc. No. 850, at 1-2.) Second, as previously described, Defendant's computer was located in Rhode Island when MediaSentry discovered the infringement in this case. (Cox Subpoena and Cox Subpoena Response, Exs. G, H.) Therefore, when MediaSentry discovered the infringement on August 10, 2004, neither MediaSentry nor the Defendant was present in Massachusetts. As such, there can be no violation of the Massachusetts law when no party was present in the Commonwealth during the activity in question.

Third, to the extent that the Massachusetts Wiretap Statute could possibly apply to this case, the nature of MediaSentry's activity did not subject it to the statute. As previously discussed, Defendant consented to MediaSentry's downloads by placing the copyrighted sound recordings in a shared folder accessible to the general public. *See Thomas-Rasset*, slip op. at 11-12 (Ex. B); *see also In re Verizon Internet Servs.*, 257 F. Supp. 2d at 267. Therefore, Defendant cannot accuse MediaSentry of violating the Massachusetts Wiretap Statute when he himself consented to the communications as a user of the peer-to-peer network.

Fourth, the Massachusetts Wiretap Statute is not implicated here because the statute only prohibits the interception of communications during transmission and the subsequent disclosure of the interception. ALM GL ch. 272, § 99(C). As discussed in connection with the Federal Wiretap Act, MediaSentry never intercepted any electronic communication during transmission but merely recorded and retained the electronic communication after it was sent directly to it.[8]

B. The Massachusetts Wiretap Statute does not provide for exclusion of evidence.

Defendant has cited no authority to demonstrate that exclusion of evidence is the remedy for any violation of the Massachusetts Wiretap Statute in a civil case. Nor can he. The plain language of the Statute makes clear that exclusion of evidence does not apply in a civil case. The Statute contains a provision for "suppression of evidence," which clearly states that a court may suppress evidence that falls under the Statute only if it involves "a defendant in a criminal trial in the court of the commonwealth." ALM GL ch. 272, § 99(P). The very next provision of the Statute contains possible remedies for violations of the Statute in a civil matter, and exclusion of evidence is not one such remedy. *See* ALM GL ch. 272, § 99(Q). Thus, Defendant's argument that this Court should suppress MediaSentry's evidence for violation of the Massachusetts Wiretap Statute is without merit.

V. There Is No Basis For Suppression In This Case.

This is a civil matter that does not involve any government action that would invoke the Fourth Amendment, and thus the exclusionary rule should not apply. As the Supreme Court explained in *United States v. Janis*, 428 U.S. 433, 447 (1976), "In the complex and turbulent

[8] To the extent that Defendant may seek to suppress the MediaSentry evidence based on an alleged violation of the Rhode Island Wiretap Statute, R.I. Gen. Laws § 12-5.1-1 *et seq.*, Defendant's motion should be denied for the same reasons set forth above. Specifically, Defendant consented and there was no interception.

history of the [exclusionary] rule, the Court never has applied it to exclude evidence from a civil proceeding, federal or state." *See Thompson v. Carthage Sch. Dist.*, 87 F.3d 979, 981-982 (8th Cir. 1996); *United States v. Tauil-Hernandez*, 88 F.3d 576, 581 (8th Cir. 1996) ("The Supreme Court has declined various invitations to extend the Fourth Amendment exclusionary rule beyond the criminal trial."). *See also Vander Linden v. United States*, 502 F. Supp. 693, 696 (S.D. Iowa 1980) ("On a number of occasions the United States Supreme Court has stated that the purpose of the exclusionary rule is to safeguard Fourth Amendment rights by deterring future and unlawful police conduct."); *Mejia v. City of New York*, 119 F. Supp. 2d 232, 254 (S.D.N.Y. 2000) ("the Fourth Amendment's exclusionary rule does not apply in civil actions other than civil forfeiture proceedings.") (*citing Pennsylvania Bd. of Probation & Parole v. Scott*, 524 U.S. 357, 363 (1998)). As this Court has held, "evidence seized by a private citizen in violation of the Fourth Amendment is admissible." *London-Sire Records*, Case No. 07CV10834-NG, slip op. at 4 (Gertner, J.).

Moreover, not one of the federal or state laws which Defendant references in his Motion to Suppress provides for the exclusion of evidence as a remedy for an alleged violation of those laws. And, in fact, the case law, and in the case of the Federal Wiretap Act, the statute itself, specifically reject suppression. *See, supra,* Argument, Sections II, B; III, B; and IV, B.

VI. Suppression For Violation Of Ethics Rules Is Unprecedented And Would Be Inappropriate Here.

Recognizing that the federal and state authorities relied upon do not support the exclusion of evidence in this case, Defendant resorts to arguing for exclusion based on the rules of ethics. Of course, Defendant has not and could not cite a single authority to support his claim that Plaintiffs or their counsel have in any way violated any rule of ethics. This argument is merely

an unfortunate, and unprofessional attack made in a desperate attempt to suppress evidence that Defendant and his counsel know is ruinous to his defense.

Leaving aside Defendant's unprofessional attack on the integrity of Plaintiffs and their counsel, which merits no further response, the cases that Defendant relies on do not support his arguments for suppression of evidence.

In *Microsoft Corp. v. Alcatel Business Systems,* No. 07-090-SLR, 2007 WL 4480632 (D. Del. 2007), evidence was excluded due to a clear violation of Model Rule 4.2. In particular, counsel spoke to an employee of a represented party without the representing attorney's consent.

Similarly, in *McIntosh v. State Farm Fire & Cas. Co.,* 2008 WL 941640 (S.D. Miss. 2008), the Court excluded evidence after it was found that the attorney encourages witnesses to disclose confidential documents and paid individuals money to encourage the misappropriation of confidential documents. As Defendant concedes, this was a clear violation of ethical rules regarding payment of material witnesses.

In *Hammond v. City of Junction City,* 167 F. Supp. 2d 1271 (D. Kan. 2001), the court excluded evidence after it found a clear and direct violation of Rule 4.2 due to plaintiff's counsel communicating ex parte with Defendant's managerial employee.

In *Aiken,* the court did not exclude evidence but simply discussed suppression in the context of warning counsel not to induce or listen to privileged communications from former employees. *Aiken*, 885 F. Supp. at 1480. The court suppressed no evidence and did not discuss the calculus for when or what evidence might be suppressed for a violation of ethical rules.

In *Trans-Cold Express v. Arrow Motor Transit, Inc.,* 440 F.2d 1216 (7th Cir. 1971), the Court excluded evidence after finding that an attorney's investigator engaged in improper ex parte communication and had mislead employees into believe that he represented the employer.

And in *Borges v. Our Lady of the Sea Corp*, 935 F.2d 436 (1st Cir. 1991), there was no exclusion of evidence. While the court did discuss exclusion, it was in response to a clear conflict of interest, in which an attorney acted as counsel for plaintiff while he was still a member of the firm engaged in active representation of the defendant in another matter.

In all of these cases, exclusion of evidence occurred, if at all, only after the court found a clear violation of an unmistakable ethical rule by a party or its representative. Here, in contrast, Defendant cites no ethics rule Plaintiffs' violated. Instead, Defendant, apparently acknowledging that the statutes at issue do not provide for exclusion, attempts to bootstrap the alleged statutory violations with unsupported claims that Plaintiffs' counsel somehow violated their ethical obligations, and therefore, there is some sort of moral imperative of exclusion. However, where the statutes and case law specifically reject exclusion, the ethics rules cannot revive it. Defendant has not cited a single case where a court, citing to any state, federal or model ethics rules, excluded evidence allegedly obtained in violation of a state private detectives licensing statute or federal or state wiretapping or eavesdropping laws.

CONCLUSION

If simply recording an IP address and metadata sent to someone over the Internet was illegal, copyright holders would be unable to protect their content on the Internet. Defendant used the KaZaA peer-to-peer file sharing program to download and distribute Plaintiffs' copyrighted sound recordings. The recordings in Defendant's shared folder could have been downloaded by any one of the millions of users of the FastTrack network. MediaSentry was one of those users and, and instead of simply downloading the copyrighted sound recordings from Defendant, it downloaded the files and recorded the metadata and transmission data associated with those files as they were sent from Defendant to MediaSentry.

WHEREFORE, Plaintiffs ask that the Court deny Defendant's motion to suppress evidence. Respectfully submitted this 7th day of July, 2009.

SONY BMG MUSIC ENTERTAINMENT; WARNER BROS. RECORDS INC.; ATLANTIC RECORDING CORPORATION; ARISTA RECORDS LLC; and UMG RECORDINGS, INC.

By their attorneys,

By: s/ Eve G. Burton

Timothy M. Reynolds (pro hac vice)
Eve G. Burton (pro hac vice)
Laurie J. Rust (pro have vice)
HOLME ROBERTS & OWEN LLP
1700 Lincoln, Suite 4100
Denver, Colorado 80203
Telephone: (303) 861-7000
Facsimile: (303) 866-0200
Email: eve.burton@hro.com

Daniel J. Cloherty
DWYER & COLLORA, LLP
600 Atlantic Avenue - 12th Floor
Boston, MA 02210-2211
Telephone: (617) 371-1000
Facsimile: (617) 371-1037
dcloherty@dwyercollora.com

ATTORNEYS FOR PLAINTIFFS

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non-registered participants on July 7, 2009.

s/ Eve G. Burton