

LAW OFFICES OF  
THOMAS M. MULLANEY  
708 THIRD AVENUE, SUITE 2500  
NEW YORK, NEW YORK 10017  
Tel.: (212) 223-0800  
Fax: (212) 661-9860

February 27, 2008

**BY REGULAR MAIL AND ECF**

Hon. Robert M. Levy  
United States Magistrate Judge  
United States District Court  
225 Cadman Plaza East  
Brooklyn, NY 11201

Re: UMG Recordings, Inc., et al. v. Lindor  
05-Cv-1095 (DGT)(RML)

Dear Magistrate Judge Levy:

I write on behalf non-party SafeNet, Inc, f/k/a MediaSentry, Inc. ("SafeNet") in opposition to the letter application of Ray Beckerman, Esq., dated February 19, 2008 moving to compel the production of documents responsive to Document Requests no. 1-3, and 5-28 (Mr. Beckerman having withdrawn no. 29). SafeNet respectfully asserts that, in a case where the sole remaining contention appears to be that Defendant Lindor was not actually the individual operating her computer when it was used by a jrlindor@KaZaA to illegally distribute music files, a subpoena propounding twenty eight (28) document requests, exclusive of numerous sub-parts, is overly-broad and unduly burdensome on its face. Defendant has also failed to demonstrate her need for the highly sensitive and confidential information sought, from a non-party, to present a defense.

Defendant's counsel attempts to obfuscate the simple facts of this case by erroneously claiming that SafeNet has improperly withheld responsive documents. Contrary to what Defendant represents to the Court, however, every document relevant to the Lindor litigation that SafeNet ever generated was produced to her long ago. Instead, it was her counsel who insisted that SafeNet not produce to her the "Lindor file," precisely because it had already been produced by Plaintiffs. Complying with her counsel's demands does not constitute a fair basis for subsequent motion practice against SafeNet.

It has long been asserted in this case, without dispute, that SafeNet provided every document relevant to the Lindor "capture" to the Plaintiffs, the so-called "Lindor file", who in turn provided them to Defendant on April 8, 2006. The Lindor file consists of hundreds of pages of documents, and

includes a host of technical documents -- and all of the technical documents relevant to this case. If Defendant's counsel has changed his mind and would like another copy of the Lindor file, SafeNet would be happy to oblige.

The true purpose of Defendant's motion is to extract and expose highly sensitive, proprietary information that far exceeds the scope of this case, for reasons unrelated to her individual defense. A review of the docket sheet demonstrates that the pending application is not the first attempt by defendant to do so, which Your Honor has rebuffed already. On March 30, 2007 this Court denied Defendant's motion to compel the production of certain documents reflecting the contractual relationship between the Recording Industry Association of America and SafeNet, as those confidential, proprietary documents were not likely to lead to the discovery of admissible evidence.

Moreover, Defendant herself has stated that the information now sought from SafeNet is proprietary and confidential. E.g., Letter of Ray Beckerman to Hon. Robert M. Levy, dated March 12, 2007. In that circumstance, it is Defendant's burden to demonstrate her need for SafeNet's proprietary and confidential information. E.g., Four Star Capital Corp. v. Nynex Corp., 183 F.R.D. 91, 110 (S.D.N.Y.). Her counsel's conclusory, and entire, argument that the information sought is "clearly needed to evaluate the integrity of MediaSentry's methods, and the basis for its trial exhibits" does not satisfy that burden.

How Defendant's newly-developed need for production of all of SafeNet's source code, for example, would lead to admissible evidence is left unsaid, probably because it would reveal not only all of the information found problematic by the Court on March 30, but a font of even more sensitive and less relevant proprietary information belonging to a non-party. In fact, Defendant's document requests effectively ask for every page and line of SafeNet's internal techniques, processes and procedures for every facet of the former-MediaSentry's internet security business, whether or not related to Defendant, the KaZaA network, or even the record industry. See, e.g., Document Requests No. 6-7, 9-11, 14-18, 21-22.

A party to a litigation seeking source code and similar proprietary technical documents from a non-party has an especially high burden to satisfy before obtaining such material. Bell Atlantic Business Sys. Svcs., Inc. v. Hitachi Data Sys. Corp., 1995 WL 13115 (S.D.N.Y.1995)(court denied motion to compel production of non-party's source code because "no protective order could possibly be devised which could guarantee [its] security"). Even as to parties, it is well-established that a party seeking another's source code must make a significant showing of need for that sensitive information, which would then be made available only under very strict conditions to protect that information. E.g., Member Svcs., Inc. v. Security Mut. Life Ins., 2007 WL 2907520 (N.D.N.Y. 2007)(expert affidavit required to show need for source code, which could not be disclosed to party or its counsel).

Defendant here has made no showing of need, has not sought this information for the three years this case has been pending, has not shown that she has exhausted other means of obtaining the desired evidence, and has refused to even discuss an appropriate Protective Order. Even if SafeNet were a party to this case, and the litigation alleged that SafeNet had infringed defendant's software patent, its source

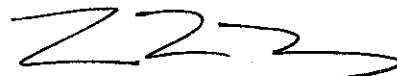
code and other software architecture documents would be protected from discovery with Ms. Lindor's deficient showing. *See New York University v. E.piphany, Inc.*, 2006 WL 559573 (S.D.N.Y 1996) (LTS)(RLE) (plaintiffs must demonstrate that they have exhausted others means of attempting to prove patent infringement before obtaining any component of source code). As against a non-party, and asserting a defense much less complicated than patent infringement, defendant's motion to compel is baseless.

Moreover, defendant's counsel, the author of a blog entitled "Recording Industry vs People", that he proudly describes as vitriolic, also appears disconcertingly eager to obtain this information without the encumbrance of an appropriate Protective Order. In that blog, Defendant's counsel accuses Plaintiffs' attorneys and MediaSentry of fabricating evidence, among other crimes and improprieties, and there seems to be strong reason to believe that he has violated a previous Protective Order in this case by disseminating Confidential deposition testimony. Plaintiff's Memorandum Brief in Support of Their Motion For Protective Order, dated September 27, 2006, at p.12. Defendant ought to be required to make an extraordinary showing of need for such sensitive information in this context.

Instead, Defendant can not even contend that the "integrity of MediaSentry's methods" is a legitimate issue in this case. From prior proceedings it appears that she has repeatedly taken the position that an unknown individual used her computer to infringe copyright, while conceding that her computer was the one used to do so. *Id.*, at p.9. But SafeNet has no role other than to find that computer by connecting to KaZaA users as any other user would, and then providing to Plaintiffs the internet protocol ("ip") address of the infringer, *inter alia*, from which Defendant accessed KaZaA. The internet service provider then supplies the identity of the person assigned that ip address, which is assigned just as an individual with a street address and a telephone would be assigned a telephone number. Because Defendant seems to be admitting that Plaintiff has the right street address and phone number, there is no legitimate cause to "evaluate the integrity" of the process that developed that information. That is doubly so where the ip address was assigned to defendant, Ms. Lindor, and the KaZaA infringer used the name "jrlindor."

This Court has doubtless seen hundreds of defendants before it who were eventually convicted largely or solely on recorded telephone conversations. Where a criminal defendant is recorded saying his name is Lindor, and then the pen register records show the telephone number that "Lindor" used was assigned to someone named Lindor, Courts will unlikely allow that defendant to subpoena the phone company to evaluate the integrity of its processes, because someone else named Lindor may have really been using that phone. This case is no different

Respectfully,



Thomas M. Mullaney

Cc: All Counsel of Record