UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
----------X

CAPITOL RECORDS, LLC, d/b/a
EMI MUSIC NORTH AMERICA,

Plaintiff,

-against-

ESCAPE MEDIA GROUP, INC.,

Defendant.

----------X

12-CV-06646 (AJN)(SN)

REPORT AND RECOMMENDATION

SARAH NETBURN, United States Magistrate Judge.

TO THE HONORABLE ALISON J. NATHAN:

INTRODUCTION

In 1999, a teenage college dropout finished writing software for an internet service called Napster that would allow people to swap music stored on their computers. Six months after the service was released, 18 record companies filed a lawsuit to shut it down. Since then, content-sharing websites have proliferated. Listening to music obtained free from others over the internet has become increasingly common; so too have lawsuits that pit corporate copyright owners against emergent online service providers in disputes over the use of copyrighted musical works. This is such a lawsuit.

Before the Court is the plaintiff EMI's motion for summary judgment on its copyright infringement claims against Escape Media Group, which operates the free music-streaming website Grooveshark.com. Like many recent copyright lawsuits against online service providers, this case turns not on whether Grooveshark exploits EMI's copyrighted works without

authorization, but on whether Escape can secure immunity from monetary liability for any infringing activity under the Digital Millennium Copyright Act.

After considering the papers submitted in support of and in opposition to EMI's summary judgment motion, as well as the arguments advanced by the parties at the April 29, 2014 hearing, the Court recommends that EMI's motion for summary judgment be **GRANTED IN PART and DENIED IN PART.** Specifically, the Court recommends finding that Escape, as a matter of law, is not entitled to an affirmative defense under the Digital Millennium Copyright Act, and that summary judgment should be granted in favor of EMI on its claims for direct infringement of the right of performance under federal law, secondary infringement under federal law for both contributory and vicarious infringement, and direct and secondary infringement under New York common law for copyrighted works not covered by the Copyright Act. The Court recommends that EMI's motion be denied with respect to its claim for direct infringement of its right of reproduction.

PROCEDURAL BACKGROUND

On August 30, 2012, the plaintiff, Capitol Records, LLC, d/b/a EMI Music North America ("EMI"), brought this action against Escape Media Group, Inc. ("Escape"), alleging claims for: (1) copyright infringement, in violation of the Copyright Act of 1976 (the "Copyright Act"), 17 U.S.C. § 101, *et seq.*; (2) breach of contract as to the parties' Digital Distribution Agreement; (3) breach of contract as to the parties' Settlement Agreement; (4) unjust enrichment; (5) unfair competition; and (6) common law copyright infringement. Escape answered the complaint on October 15, 2012, asserting several affirmative defenses, including that Escape is immune from EMI's copyright infringement claims under the "safe harbor" provisions of the Digital Millennium Copyright Act (the "DMCA"), 17 U.S.C. § 512, *et seq*. On

July 16, 2013, Escape stipulated to liability on EMI's claim for breach of the Digital Distribution Agreement but left open the question of damages. The Honorable Alison J. Nathan referred this matter to me for dispositive motions on October 24, 2013.

Motions for summary judgment in this action were due on December 20, 2013. Because the parties indicated that they might seek to seal portions of EMI's anticipated summary judgment motion, the Court permitted the parties to exchange their motion papers privately and then confer on the issue of a motion to seal, which the Court would resolve before allowing any motion papers to be filed on ECF.[1] On March 4, 2014, the Court received paper copies of all briefs and evidence submitted in support of and in opposition to EMI's motion for summary judgment.

In support of its motion, EMI submitted the following documents: (1) Statement of Material Facts ("SMF"); (2) Declaration of Benjamin Semel (the "Semel Declaration"), attaching Exhibits 1 through 20; (3) Declaration of Ellis Horowitz (the "Horowitz Declaration"), attaching Exhibits 1 through 13; and (4) Declaration of Alasdair McMullan (the "McMullan Declaration"), attaching Exhibits 1 through 32.

In opposition to EMI's motion, Escape submitted the following documents: (1) Response to Statement of Material Facts ("Response SMF"); (2) Declaration of Matthew Giger (the "Giger Declaration"), attaching Exhibits A through F; (3) Declaration of Samuel Tarantino (the "Tarantino Declaration"), attaching Exhibits A through E; (4) Declaration of Colin Hostert (the "Hostert Declaration"); and (5) Declaration of Cole Kowalski (the "Kowalski Declaration").

[1] On March 11, 2014, the parties emailed the Court a joint application for leave to file certain documents under seal or with redactions. The Court held a conference on that application on May 15 and issued a related order on May 16, 2014. Consistent with that order, the parties filed their motion papers on ECF on May 21, 2014.

In its reply, EMI submitted a Reply Statement of Material Facts ("Reply SMF"), and a second Declaration of Benjamin Semel (the "Reply Semel Declaration"), attaching Exhibits 1 through 11.

The parties appeared for a hearing on EMI's summary judgment motion on April 29, 2014.

DISCUSSION

I. Legal Standard

Under Rule 56 of the Federal Rules of Civil Procedure 56,[2] the Court "shall grant summary judgment if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a); see Celotex Corp. v. Catrett, 477 U.S. 317, 322-23 (1986). The moving party must show that "under the governing law, there can be but one reasonable conclusion as to the verdict." Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 250 (1986). "[T]he trial court's task at the summary judgment motion stage of the litigation is carefully limited to discerning whether there are any genuine issues of material fact to be tried, not deciding them. Its duty, in short, is confined at this point to issue-finding; it does not extend to issue-resolution." Gallo v. Prudential Residential Servs., LP, 22 F.3d 1219, 1224 (2d Cir. 1994).

The moving party "bears the initial responsibility of informing the district court of the basis for its motion" and identifying the matter that "it believes demonstrate[s] the absence of a genuine issue of material fact." Celotex, 477 U.S. at 323. The substantive law governing the case will identify those facts that are material and "[o]nly disputes over facts that might affect the outcome of the suit under the governing law will properly preclude the entry of summary judgment." Anderson, 477 U.S. at 248. "Even where facts are disputed, in order to defeat

[2] Unless otherwise noted, all "Rules" cited in this report refer to the Federal Rules of Civil Procedure.

summary judgment, the nonmoving party must offer enough evidence to enable a reasonable jury to return a verdict in its favor." Byrnie v. Town of Cromwell, Bd. of Educ., 243 F.3d 93, 101 (2d Cir. 2001).

In determining whether summary judgment is appropriate, the Court must resolve all ambiguities and draw all reasonable inferences in the light most favorable to the non-moving party. See Scott v. Harris, 550 U.S. 372, 378 (2007); Matsushita Elec. Indus. Co. v. Zenith Radio Corp., 475 U.S. 574, 587 (1986). Summary judgment is improper if there is any evidence in the record from any source from which a reasonable inference could be drawn in favor of the non-moving party. See Chambers v. TRM Copy Ctrs. Corp., 43 F.3d 29, 37 (2d Cir. 1994). To create a disputed fact sufficient to deny summary judgment, the non-moving party must produce evidence in the record and "may not rely simply on conclusory statements or on contentions that the affidavits supporting the motion are not credible[.]" Ying Jing Gan v. City of New York, 996 F.2d 522, 532 (2d Cir. 1993). "[R]ather his response, by affidavits or otherwise as provided in the Rule, must set forth specific facts demonstrating that there is a genuine issue for trial." Wright v. Goord, 554 F.3d 255, 266 (2d Cir. 2009) (citation and internal quotation marks omitted).

In addition, "the district court may not rely solely on the statement of undisputed facts contained in the moving party's [Local Civil] Rule 56.1 statement. It must be satisfied that the citation to evidence in the record supports the assertion." Vt. Teddy Bear Co. v. 1–800 Beargram Co., 373 F.3d 241, 244 (2d Cir. 2004) (citing Giannullo v. City of New York, 322 F.3d 139, 143 n.5 (2d Cir. 2003) (stating that not verifying the assertions in the Rule 56.1 statement "would derogate the truth-finding functions of the judicial process by substituting convenience for facts")). The Court of Appeals has "long recognized that [because] summary judgment is a

drastic device that cuts off a party's right to present his case to a jury, . . . the moving party bears a heavy burden of demonstrating the absence of any material issues of fact." Nationwide Life Ins. Co. v. Bankers Leasing Ass'n, Inc., 182 F.3d 157, 160 (2d Cir. 1999)) (internal quotation marks and citations omitted); see also Am. Home Assurance Co. v. ZIM JAMAICA, 418 F. Supp. 2d 537, 542 (S.D.N.Y. 2006) ("Because summary judgment is a drastic device, the movant's burden is a heavy one.").

Where, as here, "a plaintiff uses a summary judgment motion, in part, to challenge the legal sufficiency of an affirmative defense—on which the defendant bears the burden of proof at trial—a plaintiff 'may satisfy its Rule 56 burden by showing that there is an absence of evidence to support [an essential element] of [the non-moving party's case].'" Nw. Mut. Life Ins. Co. v. Fogel, 78 F. Supp. 2d 70, 73 (E.D.N.Y. 1999) (quoting FDIC v. Giammettei, 34 F.3d 51, 54 (2d Cir. 1994)) (brackets in original). See also G Investors Holding LLC v. Lincoln Ben. Life Co., Inc., 09 Civ. 2980 (ALC)(KNF), 2012 WL 4468184, at *4 (S.D.N.Y. Sept. 25, 2012) (quoting Brady v. Town of Colchester, 863 F. 2d 205, 211 (2d Cir. 1988) ("When considering a motion for summary judgment, the district courts must . . . be 'mindful of the underlying standards and burdens of proof . . . because the evidentiary burdens that the respective parties will bear at trial guide district courts in their determination of summary judgment motions.'") (internal citation omitted). A plaintiff moving for summary judgment on its affirmative claims, however, "bears a much greater initial burden; it must show that the evidence supporting its claims is so compelling that no reasonable jury could return a verdict for the defendant." SEC v. Meltzer, 440 F. Supp. 2d 179, 187 (E.D.N.Y. 2006); accord G Investors Holding LLC, 2012 WL 4468184, at *4.

II. Evidentiary Objections

In its opposition, Escape objects to the following portions of the declaration of Ellis Horowitz, EMI's expert witness: (1) statements that rely on analyses of Escape's data conducted using Copysense, software created by the company Audible Magic, on the ground that Audible Magic is functioning as an expert witness but was not disclosed properly as such; (2) data analyses and findings that EMI did not disclose timely to Escape; and (3) statements "concerning the supposed purpose or intent of Grooveshark's design and procedures." (Opp'n at 22-23.) In its reply, EMI objects to the Kowalski Declaration on the procedural ground that Kowalski was not disclosed properly as a witness and the substantive grounds that Kowalski's testimony is "diversionary," "not accurate," "unsupported by evidence," and submitted "to create a 'sham' dispute over facts." (Reply at 24-25.) For the following reasons, the Court recommends (1) overruling Escape's objections to the Horowitz Declaration, and (2) striking the Kowalski Declaration under Rule 37(c)(1).[3]

[3] The parties' evidentiary objections are based primarily on Rule 37, which generally permits a court to preclude evidence that was not produced or for which the source was not disclosed during discovery in compliance with Rule 26. Magistrate judges may rule on nondispositive pretrial matters, including discovery disputes such as requests for preclusion of undisclosed evidence under Rule 37. See Fed. R. Civ. P. 72(a); 28 U.S.C. § 636(b)(1)(A) (stating that such rulings are subject to review under a "clear error" standard"); Arista Records, LLC v. Doe 3, 604 F.3d 110, 116 (2d Cir. 2010); Thomas E. Hoar, Inc. v. Sara Lee Corp., 900 F.2d 522, 525 (2d Cir. 1990). Nevertheless, because the parties here did not file Rule 37 motions, and because the evidentiary objections are substantially intertwined with the summary judgment motion as a whole, I find it appropriate in this circumstance to recommend a disposition on these issues as part of my overall recommendation on the plaintiff's dispositive motion for summary judgment. Cf. 28 U.S.C. § 636(b)(1)(B).

A. Legal Standards for Objections to Evidence

1. Objections Based on Inadmissibility

The admissibility of evidence the parties submit in connection with a motion for summary judgment must be resolved as a threshold issue. See Fed. R. Civ. P. 56(e); Colon ex rel. Molina v. BIC USA, Inc., 199 F. Supp. 2d 53, 68 (S.D.N.Y. 2001) ("[T]he court must evaluate evidence for admissibility before it considers that evidence in ruling on a summary judgment motion.") (citing Fed. R. Evid. 104(a)). Although district courts may rely only on admissible evidence when granting a motion for summary judgment, Spiegel v. Schulmann, 604 F.3d 72, 81 (2d Cir. 2010), they have "'wide discretion in determining which evidence is admissible,'" LaSalle Bank Nat. Ass'n v. Nomura Asset Capital Corp., 424 F.3d 195, 205-06 (2d Cir. 2005) (quoting Nora Beverages, Inc. v. Perrier Group of Am., Inc., 164 F.3d 736, 746 (2d Cir. 1998)). At the summary judgment stage, district courts have discretion to consider evidence in inadmissible form, so long as the content would be admissible at trial. See Century Pac., Inc. v. Hilton Hotels Corp., 528 F. Supp. 2d 206, 215 (S.D.N.Y. 2007) aff'd, 354 F. App'x 496 (2d Cir. 2009) ("Hearsay evidence is admissible at the summary judgment stage if the contents would otherwise be admissible at trial.") (citing Santos v. Murdock, 243 F.3d 681, 683 (2d Cir. 2001)); Pathania v. Metro. Museum of Art, 11 Civ. 2119 (JMA), 2013 WL 1182076, at *19 (E.D.N.Y. Mar. 21, 2013) ("Even if an affidavit or declaration would not be admissible at trial, 'a court may consider it on a summary judgment motion if it is based on personal knowledge and sets forth facts to which the declarant could testify at trial and that would be admissible in evidence.'") (quoting Schaghticoke Tribal Nation v. Kempthorne, 587 F. Supp. 2d 389, 396 (D. Conn. 2008)); Masters v. F.W. Webb Co., 03 Civ. 6280L (DGL), 2008 WL 4181724, at *12 (W.D.N.Y. Sept. 8, 2008) ("Applying [Rule 56(e)], courts have . . . held that otherwise admissible evidence may be

'submitted in inadmissible form at the summary judgment stage, though at trial it must be submitted in admissible form.'") (quoting McMillian v. Johnson, 88 F.3d 1573, 1584 (11th Cir. 1996)).

2. Objections Based on Failure to Disclose

Before discovery, parties have a duty to make initial disclosures under Rule 26, which includes disclosing the identities of persons "likely to have discoverable information . . . that the disclosing party may use to support its claims or defenses" and the identities of persons that may present evidence as expert witnesses at trial. Fed. R. Civ. P. 26(a)(1)(A)(i), 26(a)(2)(A). After the discovery phase has begun, a party who has responded to an interrogatory "must supplement or correct its disclosure or response . . . in a timely manner if the party learns that in some material respect the disclosure or response is incomplete or incorrect, and if the additional or corrective information has not otherwise been made known to the other parties during the discovery process or in writing." Fed. R. Civ. P. 26(e)(1)(A).

Under Rule 37(c)(1), if a party fails to make these required disclosures, a district court may prohibit the party from using "that information or witness to supply evidence on a motion, at a hearing, or at a trial, unless the failure was substantially justified or is harmless." Fed. R. Civ. P. 37(c)(1). The Rule further states that, "[i]n addition to or instead of this sanction, the court, on motion and after giving an opportunity to be heard . . . may impose other appropriate sanctions," including ones that are less severe or more severe than precluding the evidence. Id. Rule 37(c)(1) is intended to "'to prevent the practice of 'sandbagging' an opposing party with new evidence.'" Haas v. Delaware & Hudson Ry. Co., 282 F. App'x 84, 86 (2d Cir. 2008) (quoting Ebewo v. Martinez, 309 F. Supp. 2d 600, 607 (S.D.N.Y. 2004)); see also Am. Stock Exch., LLC v. Mopex, Inc., 215 F.R.D. 87, 93 (S.D.N.Y. 2002) (stating that the purpose of Rule

37(c)(1) is to prevent "surprise" or "trial by ambush") (internal quotation marks omitted); Gunawan v. Sake Sushi Rest., 09 Civ. 5018 (ALC), 2011 WL 3841420, at *4 n.1 (E.D.N.Y. Aug. 26, 2011). Exclusion of evidence under Rule 37(c)(1) does not require a showing of bad faith. Design Strategy, Inc. v. Davis, 469 F.3d 284, 296 (2d Cir. 2006).

In Design Strategy, Inc. v. Davis, the Court of Appeals affirmed a district court's decision to preclude evidence that was not disclosed in accordance with Rule 26, but found that the district court "err[ed] in its determination that 'preclusion is mandatory' under Rule 37(c)(1) once 'the trial court finds that there is no substantial justification and the failure to disclose is not harmless.'" 469 F.3d at 297. The Court of Appeals found the following language from the district court to be "a correct statement of the Rule and of the court's discretion in applying it." Id. at 298.

> Given that Defendants have moved to preclude Doughty's testimony and that the [c]ourt held a telephone conference on this matter, it is not necessary to invoke Rule 37(c)(1)'s automatic sanction in order to preclude Doughty's testimony. Rather, Rule 37(c)(1) provides that "[i]n addition to or in lieu of [the automatic sanction], the court, on motion and after affording an opportunity to be heard, may impose other appropriate sanctions." The Court precludes Doughty's testimony in an exercise of this discretion.

Id. The district court's reference to "Rule 37(c)(1)'s automatic sanction" is derived from the 1993 Advisory Committee Notes to Rule 37, which the Court of Appeals found "cannot be squared with the plain language of Rule 37(c)(1)" setting forth a range of sanctions available to courts upon a motion and after affording an opportunity to be heard. Id.

The Court finds the prudent approach here is to construe the parties' requests to preclude certain witness declarations under Rule 37(c)(1) and to apply the analysis for discretionary application of an appropriate sanction prescribed by the Court of Appeals. Cf. Ritchie Risk-Linked Strategies Trading (Ireland), Ltd. v. Coventry First LLC, 280 F.R.D. 147, 156 (S.D.N.Y.

2012) ("Yet despite the seeming 'self-executing' nature of the preclusion sanction contained in the Rule, imposition of the preclusion sanction remains within the trial court's discretion.") (internal citation omitted). These applications, coupled with the parties' opportunity to be heard at the April 29, 2014 hearing, allow the Court to preclude the challenged evidence or issue other appropriate sanctions if justified by the following four factors established in Patterson v. Balsamico, which expand upon the "substantially justified or harmless" inquiry: "(1) the party's explanation for the failure to comply with the [disclosure requirement]; (2) the importance of the testimony of the precluded witness[es]; (3) the prejudice suffered by the opposing party as a result of having to prepare to meet the new testimony; and (4) the possibility of a continuance." 440 F.3d 104, 117 (2d Cir. 2006) (internal quotation marks omitted, alterations in original).[4] The Court is also guided by the observation that most courts in this district have found preclusion of evidence under Rule 37(c)(1) to be a "drastic remedy" that "should be exercised with discretion and caution," Ebewo, 309 F. Supp. 2d at 607, and "only be applied in . . . rare circumstances," Grdinich v. Bradlees, 187 F.R.D. 77, 79 (S.D.N.Y. 1999). Accord Ritchie Risk-Linked Strategies Trading (Ireland), Ltd, 280 F.R.D. at 156-57 (referring to evidence preclusion under Rule 37(c)(1) as a "harsh remedy" and citing authorities for imposing the sanction rarely and cautiously); Granite State Ins. Co. v. Clearwater Ins. Co., 09 Civ. 10607 (RKE), 2014 WL

[4] Courts in this circuit have adhered to the four factors most strictly when analyzing pre-trial motions *in limine*. See, e.g., Design Strategy, Inc., 469 F.3d at 296-97; Patterson, 440 F.3d at 117-18; Fitzpatrick v. Am. Int'l Grp., Inc., 10 Civ. 0142 (MHD), 2013 WL 5718465, at *3-4 (S.D.N.Y. Oct. 21, 2013). In the summary judgment context, however, many courts have declined to apply the four-factor test, instead focusing on whether the non-disclosure was justified and whether it was harmful or prejudicial. See, e.g., Granite State Ins. Co. v. Clearwater Ins. Co., 09 Civ. 10607 (RKE), 2014 WL 1285507, at *11 (S.D.N.Y. Mar. 31, 2014); Mobileye, Inc. v. Picitup Corp., 928 F. Supp. 2d 759, 766 (S.D.N.Y. 2013); In re Methyl Tertiary Butyl Ether Products Liab. Litig., 00 Civ. 1898 (SAS), 2014 WL 494522, at *2-4 (S.D.N.Y. Feb. 6, 2014); 24/7 Records, Inc. v. Sony Music Entm't, Inc., 566 F. Supp. 2d 305, 318-19 (S.D.N.Y. 2008). But see Haas, 282 F. App'x at 86-87 (applying the four-factor test).

1285507, at *11 (S.D.N.Y. Mar. 31, 2014). This formulation of the procedure for applying Rule 37(c)(1) is consistent with the principles embraced by the Court of Appeals in Design Strategy v. Davis and Patterson v. Balsamico.

B. Escape's Objections to the Horowitz Declaration

1. EMI's Allegedly Undisclosed Expert Testimony

In support of its summary judgment motion, EMI submits the declaration of its expert witness, Ellis Horowitz, which contains findings based on data analyses Horowitz conducted using Audible Magic software. Escape contends that Audible Magic is functioning as an expert witness whom EMI failed to disclose as required by Rule 26(a)(2). The Court thus must determine initially whether Audible Magic is an expert witness for the purposes of Rule 26(a) disclosures, and, if it is, must then determine if EMI's failure to disclose Audible Magic was either "substantially justified" or "harmless" and thus whether the related testimony should be precluded under Rule 37(c)(1).

In his declaration, Horowitz provides "a description of certain data and statistics concerning the Grooveshark system" and opines on "whether certain MP3 files [in Grooveshark's database] embodied sound recordings whose copyrights are owned by EMI."[5] (Horowitz Decl. ¶¶ 6, 77.) Horowitz states that he identified the recordings embodied in the MP3s and identified the copyright owner of those recordings by using Copysense, content-recognition software developed by Audible Magic. Horowitz explains that Audible Magic's software "is based on recognizing the unique content of an underlying audio work" and creating

[5] MP3s are digital music files "created through a process colloquially called 'ripping.' Ripping software allows a computer owner to copy an audio compact disk . . . directly onto a computer's hard drive by compressing the audio information on the CD into the MP3 format. The MP3's compressed format allows for rapid transmission of digital audio files from one computer to another . . . ." A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1011 (9th Cir. 2001).

a "psychoacoustic fingerprint," which is then matched against a "Global Rights Registry Database" to identify the copyright owner. (Id. ¶ 78 (internal quotation marks omitted).) The Global Rights Registry Database is "a large database of sound recording content submitted directly by content owners, including EMI." (Id.; see also AudibleMagic.com, Content ID Databases, www.audiblemagic.com/content-databases/ (last visited May 22, 2014) ("Audible Magic's Music Database is one of the most complete content identification registries in the world, containing recognition signatures for tens of millions of titles that are continually submitted by music studios and content owners world-wide.").)[6] In short, the Horowitz evidence submitted by EMI relies in part on Audible Magic's technology to demonstrate the fact that, and to what extent, EMI content is housed on Escape servers and streamed to Grooveshark users.

Audible Magic's software and services involving audio and visual content have been cited and described similarly in several recent cases. See, e.g., UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1012 (9th Cir. 2013) ("Audible Magic's technology takes audio 'fingerprints' from video files and compares them to a database of copyrighted content provided by copyright holders. If a user attempts to upload a video that matches a fingerprint from Audible Magic's database of forbidden material, the video never becomes available for viewing."); Arista Records LLC v. Lime Wire LLC, 06 Civ. 05936 (KMW), 2010 WL 10031251, at *6 (S.D.N.Y. Aug. 9, 2010) (defining "Fingerprinting Technology," which is

[6] Horowitz cites to the Audible Magic website in paragraph 78 of his declaration. To the extent the website's content is not in the record, the Court takes judicial notice of the information on the website under Federal Rule of Evidence 201 for the purpose of ascertaining the service Audible Magic offers. Cf. Hendrickson v. eBay, Inc., 165 F. Supp. 2d 1082, 1084, n.2 (C.D. Cal. 2001) (taking judicial notice of ebay.com as evidence of the "the nature of eBay's business"); Boarding Sch. Review, LLC v. Delta Career Educ. Corp., 11 Civ. 8921 (DAB), 2013 WL 6670584, at *1 n.1 (S.D.N.Y. Mar. 29, 2013) ("The Court generally has the discretion to take judicial notice of internet material.").

"available from commercial vendors such as Audible Magic," as "the most effective available means of content-recognition filtering based on recognizing the unique content of an underlying audio-visual work and detecting and preventing copying of that content"); Arista Records LLC v. Myxer Inc., 08 Civ 03935 (GAF)(JCX), 2011 WL 11660773, at *5 (C.D. Cal. Apr. 1, 2011) ("By running a sound file through Audible Magic's Copysense software . . . , Myxer can obtain high-level descriptive information, 'metadata,' about the particular sound recording. This information includes whether the sound recording is owned by a particular record company, and whether the copyright owner seeks to have it blocked from Myxer's Website.") (internal citations omitted); Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 518 F. Supp. 2d 1197, 1205-06 (C.D. Cal. 2007) (". . . Audible Magic has a database of approximately 6 million acoustical fingerprints of musical sound recordings. . . . Companies such as Audible Magic claim to have a database of file hashes that are known to contain copyrighted content."). Audible Magic's technology is often used by online content providers to filter out infringing content in an attempt to comply with the Copyright Act and the DMCA. See,e.g., id.; Myxer, 2011 WL 11660773, at *5; UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099, 1103 (C.D. Cal. 2009).

Given the nature of Audible Magic's services and its software Copysense, Audible Magic plainly is not an expert witness here. Contrary to Escape's characterizations, EMI did not "hire" Audible Magic and Audible Magic did not provide "testimony." (Opp'n at 11.) Audible Magic simply created Copysense, the software used by Horowitz to filter Grooveshark's database and obtain the results necessary to formulate his expert opinion. See Fed. R. Evid. 702. There is no authority to support a rule that a party must include the manufacturer of a tool used by its expert in its initial disclosures, nor could there be without, for instance, executives of calculator companies being subjected to constant depositions. Cf. Henry v. Champlain Enters., Inc., 288 F.

Supp. 2d 202, 220-21 (N.D.N.Y. 2003) (analyzing the reliability of an expert's "methodologies," including "the use of a software program" and the use of specific valuation instruments, but not inquiring into whether the manufacturers of the software or instruments are third-party experts).

Further, even if Escape's characterization of Audible Magic's services in this litigation were accurate, such services would likely "fall[] within the permissible scope of research and data collection done by third-party assistants to experts." Bd. of Trustees of AFTRA Ret. Fund v. JPMorgan Chase Bank, N.A., 09 Civ. 686 (SAS), 2011 WL 6288415, at *10-11 (S.D.N.Y. Dec. 15, 2011); see also Cedar Petrochem., Inc. v. Dongbu Hannong Chem. Co., Ltd., 769 F. Supp. 2d 269, 285 (S.D.N.Y. 2011) (finding expert testimony admissible where "the experts have based their conclusions on reliable results from tests conducted by independent consultants"). Going even further and accepting Escape's assertion that Audible Magic is a "third-party expert," it is still not clear why Escape's objection should be sustained. EMI is not submitting Audible Magic's testimony, but rather Horowitz's expert opinions, which, *arguendo*, would be found to rely on hearsay evidence from Audible Magic. This would be likely permissible under the Federal Rules of Evidence. See United States v. Mejia, 545 F.3d 179, 197 (2d Cir. 2008) ("Under Rule 703 [of the Federal Rules of Evidence], experts can testify to opinions based on inadmissible evidence, including hearsay, if experts in the field reasonably rely on such evidence in forming their opinions.") (internal quotation marks omitted); Century Pac., Inc., 528 F. Supp. 2d at 215.

Finally, Escape fails to show that it suffered any meaningful prejudice from EMI's failure to disclose Audible Magic, regardless of whether such a duty exists. Escape argues that "EMI's failure to disclose Audible Magic's analysis has manifestly prejudiced Escape, as it has prevented Escape from obtaining documents and deposing Audible Magic on a number of topics

affecting the reliability of its analysis." (Opp'n at 11.) Yet, Escape does not claim that a single MP3 file is incorrectly identified as an EMI work. Escape submits no evidence regarding its own music library and data to try to dispute the facts related to Horowitz's Audible Magic analyses. Escape's hypothetical and unsubstantiated prejudice is far from adequate to justify preclusion under Rule 37(c)(1), particularly where Escape possesses substantial information that would allow it to determine whether the Audible Magic analyses were reliable, without the need for additional depositions and document requests.

2. EMI's Allegedly Untimely Disclosure of Horowitz's Findings

Escape next argues that the Court should exclude Horowitz's analyses of Escape's data "because they were never properly disclosed by EMI in connection with Horowitz's expert report." (Opp'n at 20.) Under Rule 26(a)(2)(b), a party who has designated an expert witness for trial must provide the expert report to the opposing party. "[T]he report pertaining to the proposed opinions of an expert and their factual basis must be 'detailed and complete' . . . to ensure adequate trial preparation, including the opportunity for efficient follow-up discovery through deposition, if necessary." Lava Trading, Inc. v. Hartford Fire Ins. Co., 03 Civ. 7037 (PKC), 2005 WL 4684238, at *6-7 (S.D.N.Y. Apr. 11, 2005) (quoting Fed. R. Civ. P. 26(a)(2)(B), 1993 Advisory Committee Notes, at 160, and citing Rule 26(b)(4)(a)). EMI does not contest Escape's allegation that the disclosed Horowitz report was not "detailed and complete," but rather provides grounds for finding that, under Rule 37(c)(1), this "failure was substantially justified or is harmless." At the outset, a review of the discovery timeline with respect to the data on which Horowitz relied is necessary for the Court to assess Escape's objection.

Escape produced a database table and a hard drive containing over 500,000 MP3s from its servers in September 2013. (Reply Semel Decl. ¶ 14.) Horowitz's expert report was served on

October 25, 2013, the deadline set by the Court. (Id. ¶ 19.) On the same say, Escape produced additional database tables to EMI, including tables titled "SongFiles" and "deleted_SongFiles." (Id., Ex. 11.) On November 20, 2013, EMI produced 30 pages of documents containing Horowitz's data queries and statistical results. (Giger Decl. ¶ 8, Ex. F.) Per the Court's order, the deadline for depositions was November 22, 2013, a deadline which had been extended multiple times. On November 25, 2013, Escape deposed Horowitz. (Id., Ex. A ("Horowitz Dep.").) The morning of the deposition, EMI delivered to Escape corrected versions of some of Horowitz's charts and graphs. (Horowitz Dep. at 71:4-74:14.) On December 4, 2013, Escape produced additional database tables to EMI, including a table titled "Files," which is the complete centralized table Horowitz used to analyze Escape's MP3s. (Reply Semel Decl. ¶ 20, Ex. 10.)

Untimely expert submissions "are not admissible [at trial] unless the proponent of the evidence can demonstrate that his delay in complying with the required deadlines was 'substantially justified' or that it was harmless, that is, that it did not prejudice the other side." Lava Trading, Inc., 2005 WL 4684238, at *8 (citing Rule 37(c)(1)). Here, it appears that most, if not all, of Horowitz's untimely submissions were substantially justified, given that Escape produced database tables that were "integral to [Horowitz's] analysis" after Horowitz could have possibly included them in his expert report. (Semel Reply Decl. ¶¶ 19, 20.) In particular, Escape did not produce the full SongFiles database until October 25, 2013, the day that Horowitz's expert report was due. This database was necessary for Horowitz to run Query No. 1 and Query No. 6 of the Grooveshark database (Horowitz Decl., Ex. 7), the results of which supported several of Horowitz's conclusions (see, e.g., id. ¶¶ 24, 71, Ex. 9). Escape's argument that Horowitz failed to include in his expert report the statistical analyses he submits in his declaration, and which would have been impossible to include in the expert report because of

Escape's late data production, is unavailing. Further, any prejudice to Escape is minimal; there is no risk here of "surprise" or "trial by ambush" for the following reasons. Am. Stock Exch., LLC, 215 F.R.D. at 93 (internal quotation marks omitted). First, Horowitz's findings at issue are derived from Escape's own data and from running that data through content-recognition software. Escape had the opportunity to conduct its own analysis on its audio files and submit its findings with its opposition to show a genuine dispute of material fact, but it did not do so.[7] Second, many of Horowitz's findings that Escape seeks to exclude were produced to Escape before Horowitz's deposition, thus providing Escape the opportunity to question Horowitz and challenge these findings. Third, Escape could have, but did not, request leave from the Court to further depose Horowitz as to any findings he produced after his deposition. Cf. Design Strategy, Inc., 469 F.3d at 296 (stating that, in determining whether exclusion for untimely disclosure is appropriate under Rule 37(c)(1), district courts must consider the possibility of continuing the trial). Finally, in opposition to EMI's motion, Escape submits excerpts of the Horowitz Deposition that can be interpreted to undermine the weight of Horowitz's findings, thus further mitigating any prejudice and demonstrating that Escape had the opportunity to question Horowitz about his findings. Therefore, Escape has not shown sufficiently that Horowitz's data analyses should be stricken, and EMI has shown that any failure to comply with Rule 26(a)'s disclosure requirements was either substantially justified or harmless. The Court recommends denying Escape's objection.

[7] Escape had the ability to replicate Horowitz's analyses in order to dispute or explain his findings, as demonstrated by Kowalski's testimony that he arrived at one of his conclusions "by running the query disclosed in Mr. Horowitz's Declaration." (Kowalski Decl. ¶ 14.)

3. Expert Testimony on Purpose or Intent

Lastly, Escape asks the Court to exclude "Horowitz's proffered opinions concerning the supposed purpose or intent of Grooveshark's design and procedures." (Opp'n at 22.) Escape cites the following examples of the Horowitz Declaration as inadmissible: (1) Escape uses a database of commercial music content metadata "to ensure that the artist, album and song information is correct on Grooveshark. The apparent purpose is to curate and organize content to accurately describe commercially released recordings, so that when a user searches for [a song] . . . , that user is finding that sound recording on Grooveshark, and not something else" (Horowitz Decl. ¶ 34); and (2) "Thus, the only apparent purpose for storing these additional files is so that they may be used as a 'back up' to replace Primary Files that are removed during takedowns so that the song remains playable on Grooveshark" (Id. ¶ 58).

Horowitz is an expert in computer science and software engineering. His opinions quoted above and identified by Escape as examples of inadmissible evidence provide explanations as to why certain computer processes might be implemented. These opinions are based on Horowitz's technical expertise and would "help the trier of fact to understand the evidence or to determine a fact in issue." Fed. R. Evid. 702(a). In Arista Records LLC v. Lime Group LLC, a court in this district denied a similar objection to Horowitz's opinions concerning "intent," finding that

> Dr. Horowitz has not opined on the parties' state of mind, but rather has provided information on the *design* and *functionality* of the [MP3 streaming] program . . . . Such expert opinion is proper and aids the finder-of-fact in understanding [the website's] features. Dr. Horowitz does not make any impermissible legal conclusions, such as stating that [the defendant] actually intended to facilitate copyright infringement. He also does not cross the line into unreliable speculation about the intended purpose of various [website] design features.

784 F. Supp. 2d 398, 412-14 (S.D.N.Y. 2011). Further, unlike fact witnesses, "an expert is permitted wide latitude to offer opinions, including those that are not based on firsthand

knowledge or observation." Daubert, 509 U.S. at 592; see also Nimely v. City of New York, 414 F.3d 381, 396 n.11 (2d. Cir. 2005) (stating that "an 'expert' witness is permitted substantially more leeway than 'lay' witnesses in testifying as to opinions" that go beyond the witness's immediate perception).

In response, Escape asserts that it "explains [in its opposition brief] its actual reasons for these processes, and the Court or jury is quite capable of determining Escape's intent from primary evidence, not pseudo-'expert' opinions on what amounts to corporate psychology." (Opp'n at 22.) Escape is arguing essentially that Horowitz's testimony is insufficient to establish any facts proposed by EMI as to Escape's purpose or intent and, even if it were sufficient, the "primary evidence" would demonstrate a genuine dispute as to these material fact, which would likely result in denying EMI's motion for summary judgment. This is an argument about the merits of EMI's summary judgment motion, not about the admissibility of evidence, and is thus unnecessary to resolve here. Cf. Burch v. Regents of Univ. of Cal., 433 F. Supp. 2d 1110, 1119 (E.D. Cal. 2006) (finding objections to evidence that are "duplicative of the summary judgment standard itself" to be "redundant" and stating that, "[i]nstead of *objecting*, parties should simply *argue* that the facts are not material") (emphasis in original). Escape's objection should be denied.

C. EMI's Objection to the Kowalski Declaration

Cole Kowalski is a systems engineer who has worked for Escape since July 2011. Kowalski is responsible "for the physical maintenance of the servers that contain the [Grooveshark] databases, as well as the maintenance of Escape's database software and the 'schema' employed in various tables within databases – *i.e.*, the particular fields of data collected and maintained in those tables." (Kowalski Decl. ¶ 2.) As a basis for his declaration, Kowalski

"collected and reviewed certain data from database tables that were produced in discovery in this action." (Id. ¶ 3.) Kowalski's testimony is offered primarily to dispute EMI's proposed facts regarding Escape's affirmative defense of safe harbor under the DMCA. Escape's proposed facts supported by Kowalski's testimony include that (1) Escape has removed uploading privileges of nearly 39,000 users who submitted files associated with a DMCA takedown (Counter SMF ¶ 93); (2) Escape maintains records of every DMCA takedown processed and the submitting users (id. ¶ 98); (3) Escape processed more than 2.1 million DMCA takedowns and disabled uploading capability for numerous users between November 1, 2010 and March 20, 2012 (id. ¶ 99); and (4) Escape removes all primary and non-primary song files when processing a DMCA Lite takedown (id. ¶ 122).

1. Rule 37(c)(1)

In violation of Rule 26(a), Escape did not disclose Kowalski in its initial disclosures as a person likely to have discoverable information. (Semel Reply Decl., Ex. 8.) In violation of Rule 26(e), Escape did not disclose Kowalski in response to EMI's Interrogatory No. 1, which asked Escape to identify all persons "with knowledge of the . . . affirmative defenses set forth in the . . . Answer." (Semel Decl., Ex. 9 at 5.) Further in violation of Rule 26(e), Escape did not disclose Kowlaski in response to EMI's Interrogatory Nos. 5 or 6, which sought the identities of custodians of documents relating to the usage or exploitation of EMI content on Grooveshark.

The Court thus applies the following four factors to determine whether the Kowalski Declaration should be precluded under Rule 37(c)(1): (1) Escape's explanation for its failure to disclose; (2) the importance of Kowalski's testimony; (3) the prejudice that would be suffered by EMI as a result of having to prepare to meet Kowalski's testimony; and (4) the possibility of a continuance. Patterson, 440 F.3d at 117. First, Escape's opposition does not attempt to explain

why Kowalski was not identified in Escape's initial disclosures or in response to EMI's interrogatories, nor has Escape sought leave to file a sur-reply in light of EMI's objection. Cf. Gunawan, 2011 WL 3841420, at *4 n.1 ("Defendant's opposition brief did not address this issue [of its failure to identify a fact witness in its initial disclosures] and nor did Defendant seek leave to file a sur-reply in the face of Plaintiff's objection to the consideration of the Declarations. Because Federal Rule of Civil Procedure 37(c)(1) prohibits the use of undisclosed evidence in the absence of 'substantial justification,' those Declarations were not considered.").

At the April 29, 2014 hearing, Escape did not offer an explanation for failing to disclose Kowalski as a witness other than to assert that, because his declaration was offered to rebut or impeach Horowitz's testimony, including Kowalski in Escape's initial disclosures was not required. This explanation is untenable. Rule 26(a) requires parties to disclose "each individual likely to have discoverable information—along with the subjects of that information—that the disclosing party may use to support its claims or defenses, unless the use would be solely for impeachment." Fed. R. Civ. P. 26(1)(A)(i). The Kowalski Declaration is submitted as evidence in support of Escape's affirmative defense and to attempt to establish a dispute of material fact. Nothing in the Kowalski Declaration is offered to cast doubt on Horowitz's *credibility* and thus is not offered for impeachment purposes. Cf. Cary Oil Co., Inc. v. MG Ref. & Mktg., Inc., 257 F. Supp. 2d 751, 757 (S.D.N.Y. 2003). While Rule 26(a)(2)(D)(ii) excuses the late disclosure of rebuttal "[e]xpert [t]estimony," Kowalski has not been presented as an expert witness, making this exception inapplicable. Escape therefore has not provided a valid explanation for why it did not include Kowalski in its initial disclosures under Rule 26.

Second, because Escape cites only to the Kowalski Declaration in its Counter SMF to attempt to dispute many of EMI's proposed facts, particularly ones salient to Escape's DMCA

defense, the declaration is particularly important to Escape's opposition. Cf. Haas, 282 F. App'x at 86. Third, EMI would be substantially prejudiced were the Court to consider the Kowalski Declaration because EMI did not have the opportunity to depose Kowalski or to address his testimony in its opening summary motion papers. See id. (finding that a party's explanation for not disclosing a declarant did "not diminish the prejudice caused by waiting until after the close of discovery and, moreover, after [the moving party] had prepared and filed its motion for summary judgment"). Further, Kowalski does not submit any exhibits with his declaration and often fails to explain adequately how he reached his conclusions, thus preventing EMI from substantively responding in its reply brief.

Fourth, granting a continuance at this late stage in the litigation would be inefficient, unduly prejudicial, and an unwarranted concession to Escape for its violations of Rule 26. Fact discovery in this action initially was scheduled to close on February 22, 2013, and all fact witness depositions were to have been completed by January 30, 2013. The Court is not inclined to reopen fact discovery well over a year after it was scheduled to close, particularly given the multiple discovery extensions granted and discovery disputes resolved by the Court in the past year. A continuance, which neither party has requested, would not be justified by the circumstances. Cf. Chen v. New Trend Apparel, Inc., 11 Civ. 324 (GBD)(MHD), 2014 WL 1265916, at *20 (S.D.N.Y. Mar. 27, 2014) ("[G]ranting a continuance at this stage for purposes of allowing further expert discovery would prolong what has become a long and tortuous case history, and would reward the . . . defendants for disregarding this court's [discovery deadline] orders by imposing on the other parties at this late stage the need to invest significant time and expense . . . . This not only would undermine the court's ability to manage its schedule, but also

would impose a delay that may well have been designed to give the . . . defendants an unwarranted opportunity to forestall resolution of [the summary judgment] motion.").

In sum, Escape has provided no justification for its repeated failure to disclose Kowalski, despite its obligation to do so, and its non-disclosure would not be harmless. While preclusion of evidence not disclosed in compliance with Rule 26 is a drastic remedy that should be imposed sparingly, the circumstances here warrant such a remedy. In addition to addressing Rule 37(c)(1)'s concern with parties circumventing Rule 26 and "sandbagging" the opposing party with new evidence, preclusion here is also necessary to prevent Escape from circumventing what in this circuit is known as the "sham affidavit rule." Under this rule, the non-moving party to a summary judgment motion is estopped from creating disputes of material fact through declaration testimony that contradicts the declarant's prior deposition testimony. See In re Fosamax Products Liab. Litig., 647 F. Supp. 2d 265, 281 (S.D.N.Y. 2009). Allowing such declarations "would greatly diminish the utility of summary judgment as a procedure for screening out sham issues of fact." Palazzo ex rel. Delmage v. Corio, 232 F.3d 38, 43 (2d Cir. 2000) (internal quotation marks omitted). By the same principle, Escape should not be able to shield a witness from deposition by failing to disclose his identity in initial disclosures and in response to interrogatories, and then offer his uncorroborated declaration testimony as the sole supporting evidence to create multiple disputes of material facts. This principle is particularly applicable here because Kowalski's declaration adds very few, if any, new facts based on his personal experience as an Escape employee for 31 months or based on recent events involving Kowalski. Rather, his testimony consists almost exclusively of conclusions he drew from analyzing data collected for the sole purpose of opposing summary judgment, including various statistics and broad statements about Escape's practices for which he provides no supporting

evidence and threadbare, if any, explanations of how he arrived at his conclusions. Further, these conclusions are not corroborated by the extensive deposition and declaration testimony of the people Escape did list in its disclosures and interrogatory responses as being knowledgeable about the relevant subjects.[8] For these reasons, preclusion is the only appropriate and equitable remedy under Rule 37(c)(1). The Court therefore recommends that the Kowalski Declaration be stricken in its entirety.

2. Admissibility

In the alternative, even if the Court declined to strike the Kowalski Declaration under Rule 37(c)(1), it would find that a substantial portion of Kowalski's testimony is inadmissible as lay witness testimony under Federal Rule of Evidence 701 and would be required to meet the standard for expert testimony under Federal Rule of Evidence 702 for admission. See Fed. R. Civ. P. 56(e) ("Supporting and opposing affidavits shall be made on personal knowledge, shall set forth such facts as would be admissible in evidence, and shall show affirmatively that the affiant is competent to testify to the matters stated therein."); Hollander v. Am. Cyanamid Co., 172 F.3d 192, 198 (2d Cir. 1999) (holding that a district court may "strike portions of an affidavit that are not based on the affiant's personal knowledge, contain inadmissible hearsay or make generalized or conclusory statements").

[8] It is particularly notable that the facts alleged by Kowalski were not provided or corroborated by Colin Hostert, Escape's Chief Information Officer and DMCA Agent, whom Escape disclosed as having information about uploading and streaming music on Grooveshark and information about "Escape's policies and practices with respect to its compliance with the DMCA, including . . . Escape's receipt of and response to DMCA 'takedown notices,'" (Semel Reply Decl., Ex. 8 ¶ 6), and who was disclosed as the custodian for the data maintained on Escape servers "concerning the audio streaming and other usage or exploitation of recordings on or through the Grooveshark Service," (id., Ex. 9 at 7). Nor are the key facts alleged by Kowalski corroborated by Hostert in his deposition testimony in this action, his deposition testimony in a previous action, or his declaration submitted in opposition to EMI's motion for summary judgment.

Lay opinion testimony under Federal Rule of Evidence 701 is permissible when that testimony "result[s] from a process of reasoning familiar in everyday life." United States v. Rigas, 490 F.3d 208, 224 (2d Cir. 2007) (internal quotation marks omitted). This standard is fact-specific with respect to the experience and role of the person proffering the testimony. An employee whose duties included undertaking an investigation into his employer's practices, for instance, can offer opinion testimony as to that investigation. This situation arose with respect to a bank employee in Bank of China, New York Branch v. NBM LLC, in which the Court of Appeals found, "The fact that [the employee] has specialized knowledge, or that he carried out the investigation because of that knowledge, does not preclude him from testifying pursuant to Rule 701, so long as the testimony was based on the investigation and reflected his investigatory findings and conclusions, and was not rooted exclusively in his expertise in international banking." 359 F.3d 171, 181 (2d Cir. 2004). Thus, the court concluded, to the extent that the employee's "testimony was grounded in the investigation he undertook in his role as a Bank of China employee, it was admissible pursuant to Rule 701 of the Federal Rules of Evidence because it was based on his *perceptions*." Id. at 181-82 (emphasis in original). Had the employee's testimony not been "'a product of his investigation, but rather reflected [his] specialized knowledge,' then it was impermissible expert testimony." Rigas, 490 F.3d at 224 (quoting Bank of China, 359 F.3d at 182); see also Disability Advocates, Inc. v. Paterson, 03 Civ. 3209 (NGG)(MDG), 2008 WL 5378365, at *17 (E.D.N.Y. Dec. 22, 2008). Similarly, in United States v. Rigas, the Court of Appeals found that a former company accountant, though possessing the specialized knowledge to testify as an expert, could testify properly as a lay witness about the company's books because the testimony was based on his observations during his 20 months as a company employee. 490 F.3d at 224.

Much of Kowalski's testimony would be inadmissible unless offered as expert testimony under Federal Rule of Evidence 702, and then only if he were disclosed properly as an expert and satisfied the reliability requirements for expert testimony. See Bank of China, 359 F.3d at 182. Kowalski offers testimony as to an investigation he conducted for the sole purpose of rebutting EMI's motion for summary judgment. (See Kowalski Decl. ¶ 3 (stating that his testimony was based on his review of the discovery produced to EMI in this action).) His conclusions were derived by running calculations and processes that he would not have otherwise run as an employee and using data that is only relevant because it is what was produced to EMI in discovery. Indeed, Kowalski offers testimony intended specifically to pit his calculations and analyses against those of Horowitz, EMI's expert witness, including testimony based on replicating one of Horowitz's data queries. (See Kowalski Decl. ¶¶ 7-8, 14, 16.) Federal Rule of Evidence 701(c) "prohibits testimony from a lay witness that is 'based on scientific, technical, or other specialized knowledge'" in order "'to eliminate the risk that the reliability requirements set forth in Rule 702 will be evaded through the simple expedient of proffering an expert in lay witness clothing.'" Rigas, 490 F.3d at 224 (quoting Fed. R. Evid. 701, Advisory Committee Note to 2000 Amendment). Kowalski's testimony is based on his specialized knowledge, not on his personal perception or observations as an Escape employee. Thus, in addition to striking the Kowalski Declaration under Rule 37(c)(1), the Court recommends excluding it from consideration as inadmissible expert testimony under Federal Rule of Evidence 701.

III. Facts

A. Uncontroverted Facts

The following facts are supported adequately by admissible evidence and are admitted without controversy for the purposes of this summary judgment motion. See Local Civ. R.

56.1(c), (d) (stating that facts not "specifically controverted" in the non-moving party's counter-statement of material facts "will be deemed to be admitted for purposes of the motion"); Fed. R. Civ. P. 56(e)(2) (stating that where a party fails to address another party's assertion of fact properly, the court may "consider the fact undisputed for purposes of the motion").

1. Operation and Functionality of Grooveshark.com

Escape, founded in 2006 by Samuel Tarantino (now President and CEO) and Joshua Greenberg (now Chief Technology Officer), developed, owns, and operates an internet-based music streaming service called Grooveshark,[9] which is accessible at www.grooveshark.com ("Grooveshark.com" or "Grooveshark"). According to Tarantino, one of Escape's goals in creating Grooveshark was to make music available free of Digital Rights Management – commonly known as "DRM" – technology, which is used by major record labels to prevent copyright infringement. (See Semel Decl., Ex. 7 (Tarantino Dep.) at 47:24-48:8.) Users of Grooveshark, after accepting Escape's Terms of Service,[10] can create free accounts and submit digital MP3 files to be uploaded to a central library of sound recordings maintained on Escape's

[9] "'Streaming' generally involves compressing a file to a size small enough to be transmitted over the Internet and then allowing the receiving computer to start playing packets of the file while the remaining packets are being transmitted." WPIX, Inc. v. ivi, Inc., 691 F.3d 275, 284 (2d Cir. 2012) (quoting Preston Gralla, How The Internet Works 229-31 (7th ed. 2004). Streaming allows the user to play the recording only; it does not allow the user to download the recording, i.e., create a permanent digital file of the recording on the user's computer. United States v. Am. Soc'y of Composers, Authors & Publishers, 485 F. Supp. 2d 438, 441-422 (S.D.N.Y. 2007); Tarantino Decl. ¶ 5.

[10] Under Escape's Terms of Service, a user creating a Grooveshark account must, among other provisions, agree to the following:

> [U]nless EMG indicates otherwise, by submitting User Content to the Service you grant EMG and its affiliates a nonexclusive, royalty-free, perpetual, irrevocable, and fully sub-licensable right to use, display, perform, reproduce, publish, and distribute such User Content throughout the world via the Service. You also grant each User of the Service a nonexclusive license to access your User Content through the Service, and to use, reproduce, distribute, display, broadcast and perform such User Content as permitted through the functionality of the Service and pursuant to this Agreement.

(SMF ¶ 81.)

internet servers. Grooveshark's library is searched and displayed to users primarily using three metadata fields: Artist, Album and Song.[11] Anyone can access Grooveshark.com, search its library for particular songs, and stream music without registering an account or providing personal information. Escape streams files to users by storing a single master copy of each file in its central library and allowing multiple users to share access to that same file.

Using software provided and controlled by Escape, Grooveshark account-holders can submit their MP3s, which are then indexed and organized automatically by Escape. Only files that have metadata entries for the artist, album, and song names can be uploaded to Grooveshark. Before an MP3 is uploaded, it is run through Escape's content filtering system, which can block certain files due to their prohibited content or because the user submitting the file has had her uploading privileges revoked. The account-holder also must click a box before submitting files to verify that she understands the Terms of Service and is "only uploading content that does not infringe upon the rights of others." (SMF ¶ 83.) Tarantino acknowledges that, for at least some period, "the great majority of content" on Grooveshark came "from illegal networks," which Tarantino was "trying to monetize." (SMF ¶ 32 (quotations from attorney's statements with which Tarantino agreed).)

Escape controls what content is housed in the Grooveshark library and can block files based on their metadata or their audio fingerprints (information identifying the audio content of the files based on the way the recordings actually sound). Once an account-holder has successfully uploaded an MP3 to Grooveshark.com, she personally cannot remove that file from the website or edit the file's description or metadata. An account-holder can select an option on

[11] Metadata, often described as "data about data," is, in this context, information stored electronically in a digital audio file that describes aspects of that file, such as its name, format, size, or other information that can be entered manually. See R.F.M.A.S., Inc. v. So, 271 F.R.D. 13, 45, n.111 (S.D.N.Y. 2010).

the website to deactivate her account, but Escape has no procedure for removing account-holders' content from the Grooveshark library upon deactivation.

2. Escape's Storage and Organization of Grooveshark.com Audio Content

Escape uses its servers to house and stream MP3 files submitted by Grooveshark users. Through a technology called "fuzzy matching," which is applied without users' participation, Escape changes the metadata entered by users in order to group together content with similar but not identical names and multiple files that appear to contain the same sound recording. To further organize the content submitted by users, Escape downloads to its servers and syncs its audio library to a third-party database of commercial music content metadata called MusicBrainz. If metadata associated with Grooveshark content is found to be similar enough to listings in MusicBrainz, the MusicBrainz data replaces the data in the Grooveshark library. Escape also maintains metadata filters that allow it to block content based on artist, album, and song names, and to exclude duplicative content, i.e., content for which the audio fingerprint matches a fingerprint already in the Escape database. Escape records uniformly all file submissions in its Users_Files database table regardless of how Escape handles the content after it is submitted.

MP3 files containing the same song submitted by multiple users are grouped together, but only one file, designated the "primary file," appears in searches and will be streamed when selected by a user.[12] The files containing the same song that are not designated as the primary file (the "non-primary files") can be neither streamed nor accessed through a search.

[12] The primary files are organized by region, so the primary file played for a user in the United States will be different than one played for a user in another country.

3. Escape's Policies and Practices Regarding Infringing Works Uploaded to Grooveshark.com

With respect to user-submitted content alleged by a copyright owner to be infringing, Escape implements what it calls its "one strike policy." Through this policy, Escape purports to disable the uploading capabilities of a user after receiving one DMCA notice asserting that the user uploaded infringing content, in addition to removing the file and sending an email notification to the submitting user.[13] Although Escape has no policy to identify repeat infringers, Escape avers that its one strike policy precludes the possibility of repeat infringers. (SMF ¶ 91; Counter SMF ¶ 91; Hostert Dep. 137:21-138:7.) When Escape receives a takedown request that it considers non-compliant with the DMCA's requirements for such notifications or otherwise deems ambiguous or unofficial, Escape applies a policy it created called "DMCA Lite," under which the file is removed but the user who submitted the file does not lose her uploading privileges, does not receive a notification email, and is not recorded. An Escape database titled "Takedown Batches" shows that, since the earliest entry on February 13, 2013, 94.2% of the takedowns have been recorded in the "dmca_lite" field, as opposed to the "dmca" field.

Escape has no procedure for terminating a user's account in connection with a DMCA takedown and has never terminated a user's account for infringement. Escape has no procedure for terminating, limiting, or restricting any functionality in a user's account beyond disabling uploading privileges, regardless of how many DMCA takedown notices the user receives. Additionally, Escape has never removed from Grooveshark.com all content or data associated with an infringing user's account under a repeat infringer policy, nor does Escape have a

[13] The DMCA requires service providers to designate an agent to receive notifications of claimed infringement, which trigger the obligation for the service provider to remove the infringing content. 17 U.S.C. § 512(c)(2-3). These notifications of infringement are commonly known as DMCA "takedowns" or "notices."

procedure for removing from its library all content submitted by a user who has received repeated notices of infringement. After identifying an infringing user, Escape has no policy to, and has never attempted to, block that infringing user from creating a new Grooveshark user account. Escape does not keep an independent record of when users receive multiple DMCA takedown notices.

Between November 1, 2010, and March 20, 2012, Escape did not process or record any DMCA takedowns or disable any users' uploading capabilities in connection with DMCA takedowns. Escape does not have a policy or procedure through which it attempts to discover whether users are uploading content after receiving a DMCA takedown or whether a user who receives a DMCA takedown had received prior DMCA takedowns for previously submitted files. Additionally, when processing a DMCA takedown for an MP3 file, Escape makes a record of the infringement for the first user to submit the file only; it does not make a record for any users who submitted the infringing file afterward. In connection with this litigation, Escape produced no copies or records of DMCA notifications sent to Grooveshark users between November 16, 2010, and February 1, 2013. Escape's database table used to log DMCA takedowns contains no entries from October 31, 2010 through March 20, 2012.

Escape removes primary files from its system only in response to a DMCA takedown. Escape processes takedowns only when the copyright owner identifies the specific web address for the infringing song.[14] Web addresses are available for the primary file only; content-owners submitting takedown notices cannot obtain web addresses for non-primary files. Because the primary file exclusively is streamed and located through a search for the associated song, it is

[14] The web address for a song is an extension of the web address for the Grooveshark homepage and will look like, for example, http://grooveshark.com/s/Hello+Zepp/4dTNhl?src=5. (See Semel Decl., Ex. 17.) Escape will not remove files pursuant to a DMCA takedown if only the album web address is provided; a copyright owner must refer to the specific song web address. (Id.)

only the primary file that is identified in a takedown notice and that Escape will remove from its system. The non-primary files grouped together for that song are not removed, and Escape takes no action against and makes no record for any of the users who uploaded the non-primary files of the infringing song. After Escape removes a primary file for a song, one of the non-primary files for the song will automatically replace it, becoming the new primary file when a user selects that song for streaming, unless that song has no associated non-primary files. When a file is removed pursuant to a DMCA takedown, Escape has no policy or procedure for preventing that specific MP3 file, identified by its unique internal number called a "file hash," from reappearing on its system. According to Tarantino, Escape has implemented a policy for removing files at the request of the user who submitted the files. Tarantino estimates that Escape has removed over 18,000 files in response to requests from the submitting user.

4. The EMI–Escape Relationship

EMI owns or has the exclusive right in the United States to enforce copyrights in 2,807 sound recordings, 2,579 of which were first fixed on or after February 15, 1972, and 228 of which were first fixed before February 15, 1972.[15] On May 8, 2009, EMI sued Escape for copyright infringement and unauthorized exploitation of EMI's copyrighted sound recordings. Capitol Records, LLC, et al. v. Escape Media Group, Inc., 09 Civ. 04458 (LMM) (S.D.N.Y. May 8, 2009). The parties settled the lawsuit through the execution of two contracts effective as of September 24, 2009: the Settlement Agreement and Mutual Release (the "Settlement Agreement") and the Digital Distribution Agreement (the "Distribution Agreement").

[15] Under the Copyright Act, sound recordings are treated differently depending on whether they were "first fixed" before or after February 15, 1972. See 17 U.S.C. § 301(c) ("With respect to sound recordings first fixed before February 15, 1972, any rights or remedies under the common law or statute of any State shall not be annulled or limited by this title until February 15, 2067.").

In the Settlement Agreement, the parties set out the terms of Escape's future conduct with respect to EMI's copyrighted recordings:

> From and after the date hereof, Escape Media shall not allow the copying, reproduction, distribution, public performance, and/or other exploitation of EMI Recordings on, via, and/or in connection with the Grooveshark Sites, and/or any other website, server, system, or software under the control of Escape Media and/or an affiliate of Escape Media on which can occur the unauthorized copying, reproduction, distribution, public performance, downloading, and/or other exploitation of EMI Recordings (each, a "Comparable Service"), except pursuant to a valid and binding agreement allowing such copying, reproduction, distribution, public performance, and/or other exploitation of EMI Recordings (an "EMI Content Agreement"), in accordance with the terms of such EMI Content Agreement.

(SMF ¶ 16; McMullan Decl., Ex. 2 (Settlement Agreement).) Simultaneously to the execution of the Settlement Agreement, the parties executed the Distribution Agreement, which granted Escape the right to distribute digitally EMI's content on Grooveshark and established Escape's rights and obligations in connection with that license. Specifically, Escape agreed that "use of EMI Content obtained from any entity other than EMI or an Approved Source is a material breach of this Agreement." (SMF ¶ 19; McMullan Decl., Ex. 3 (Distribution Agreement).) The Distribution Agreement provided that, through EMI's digital supply chain, it would provide to Escape "EMI Content," defined as "any . . . materials containing any content made available by EMI to Distributor [Escape] owned or controlled by EMI." (Id.) In exchange for the rights described in the Distribution Agreement, including the right to feature EMI content on Grooveshark, Escape agreed to make certain payments and to produce regular sales reports, consisting of monthly accounting statements and weekly exploitation reports. The Distribution Agreement had an expiration clause stating that the Agreement, unless terminated earlier, would expire 30 months after the date of execution, September 24, 2009.

The terms of EMI's release are described in paragraph 5.1 of the Settlement Agreement and paragraph 12 of the April 21, 2011 amendment to the Settlement and Distribution Agreements. Under the Settlement Agreement, EMI released Escape for liability "from the beginning of time to the present, through the effective date of this Agreement, solely relating to allegedly infringing or unauthorized use or exploitation of EMI recordings on, via, and/or in connection with the Grooveshark Sites and/or the Grooveshark service." (Settlement Agreement ¶ 5.1.) Under the April 21, 2011 amendment, EMI released Escape on all claims of liability for "the Content/Usage/Accounting Claim for all periods prior to and including December 31, 2010, excepting only claims arising under this Amendment." (Tarantino Decl., Ex. D ¶ 12.)

During the term of the Distribution Agreement, EMI notified Escape twice that Escape was in breach of the Distribution Agreement due to, first, Escape's exploitation of EMI recordings that were not authorized under the Agreement and, second, Escape's failure to produce the weekly and monthly sales reports as set forth in the Agreement. EMI and Escape resolved these disputes by executing two amendments to the Settlement and Distribution Agreements, one on April 21, 2011, and the other on November 29, 2011. These amendments altered the terms of the payment provisions of the original agreements and extended the term of the Distribution Agreement through September 30, 2012. Escape, however, breached the amended Distribution Agreement by failing to render any monthly payments or sales reports to EMI as of December 2011, which prompted EMI to send Escape a notice-of-breach letter on January 25, 2012.

On March 22, 2012, EMI sent Tarantino a letter stating that EMI was terminating the Distribution Agreement because of Escape's material breach and failure to cure the breaches listed in the January 25 letter. In addition to Escape's continued failure to submit the sales

reports and monthly payments, EMI asserted that Escape failed to make the single lump payment that the parties agreed to under the second amendment to the Distribution Agreement. In the termination letter, EMI demanded that Grooveshark stop any exploitation of EMI content immediately, destroy all EMI content in its possession, and remit the outstanding payments. Following these demands in the letter, EMI noted "that any further exploitation of EMI Content is infringing and breaches the now terminated Distribution Agreement as well as the . . . settlement agreement[.]" (McMullan Decl., Ex. 6 at 2.) Though the Distribution Agreement was terminated by EMI's March 22, 2012 letter, the Settlement Agreement remains in effect.

5. Grooveshark Data Related to EMI Content

Since EMI terminated the Distribution Agreement on March 22, 2012, Escape has had no authorization to copy, stream, or otherwise exploit any rights in EMI recordings. Escape has retained in its database the fingerprints and metadata for the EMI content it had obtained through a license. Since the summer of 2011, Escape has generated fingerprints for all content on Grooveshark and all newly submitted content, which, in the past, it would match against EMI content.[16] Between March 23, 2012, and October 2013, EMI's post-1972 copyrighted recordings have been streamed on Grooveshark 10,705,193 times and have been uploaded to Escape's servers in 8,996 distinct files, and EMI's pre-1972 copyrighted recordings have been streamed on Grooveshark 1,519,374 times and have been uploaded to Escape's servers in 4,859 distinct files. In the 20 months after the Distribution Agreement was terminated, Escape logged a total of 36,603 files removed through its DMCA process – fewer than the 56,740 files removed during one month when the Distribution Agreement was in effect (October 2010).

[16] Because of the conflicting evidence regarding this fact, it is expanded upon in section III(B)(2), infra, in connection with paragraph 75 of EMI's statement of material facts.

6. Grooveshark Data for All Content

Escape's internal projections estimate that 84.5% of the streams from Grooveshark.com are of works belonging to the major labels with which Escape has no license. In analyzing Escape's records, Horowitz found the following relevant statistics:

- There are 3,323 Grooveshark users recorded for infringement who did not have their uploading privileges revoked.
- Escape has recorded 364,318 files removed by DMCA takedowns and 37,987 users who submitted files removed by DMCA takedowns.
- Users who have been recorded for infringement account for 22,066,555 file submissions, or 47% of the total file submissions in Escape's active library, and 9,837,931 uploads (defined as the first record of submission for a file), or over 48% of all uploads to Escape's active library. There are 568 users who have been recorded for infringement in connection with over 100 different recordings.
- Fourteen Escape employees have been recorded in connection with DMCA takedowns of infringing content – 13 in connection with multiple works. Four of these employees were recorded in connection with over 100 works, including Tarantino with 105 works and Greenberg with 687 works.
- There are 1,609 users who were recorded for a DMCA takedown of an upload that occurred after the user had already received a prior DMCA notice of infringement from Escape. These 1,609 users have submitted 2,339,671 files that are still available in Grooveshark's active library.

B. Insufficiently Supported Facts

Escape has not provided evidence sufficient to raise disputes as to any material facts proposed in EMI's statement of material facts. Nevertheless, the following facts proposed by EMI are not established by the evidence to which EMI cites in support of the proposed fact. In an exercise of discretion, the Court determines below whether EMI's proposed facts are otherwise established and undisputed by any evidence submitted by the parties.[17]

[17] The Court is under no obligation to sift through evidence that is not cited specifically to support a fact proposed in a statement of material facts. Indeed, "'[j]udges are not like pigs, hunting for truffles buried in the record.'" Gonzalez v. K-Mart Corp., 585 F. Supp. 2d 501, 503 (S.D.N.Y. 2008) (quoting Albrechtsen v. Bd. of Regents of the Univ. of Wis. Sys., 309 F.3d 433, 436 (7th Cir. 2002)) (deeming a

1. SMF Paragraph 54

EMI submits the material fact that "Escape uses its servers to make copies of and stream files submitted by Grooveshark users." (SMF ¶ 54.) To support this proposed fact, EMI cites to the Horowitz Declaration; portions of a deposition taken of former Escape employee Edwin Fuquen in a separate and ongoing action, UMG Recording, Inc. v. Escape Media Group, Inc. et al, 11 Civ. 08407 (TPG) (S.D.N.Y. November 18, 2011) (Semel Decl., Ex. 4); and a portion of the Hostert Deposition (id., Ex. 1). This evidence does not support EMI's assertion that Escape "make[s] copies of . . . files submitted by Grooveshark users." Rather, the evidence supports the description provided by EMI's expert, Horowitz: "[U]sers provide or 'seed' MP3 files to [Grooveshark's] central library," after which Escape's database system determines which files to accept and "stores all the files on its servers, and indexes [and] organizes . . . these files and music embodied in the files." (Horowitz Decl. ¶ 26.) Although Escape has provided no evidence to dispute EMI's proposed fact (see Counter SMF ¶ 54), the Court finds that EMI has not submitted evidence sufficient to establish that Escape makes copies of the files submitted by Grooveshark users.

2. SMF Paragraph 75

EMI submits the following material fact that is supported insufficiently by the cited evidence and that Escape purports to dispute: "Content matching the fingerprints of EMI content was blocked until EMI terminated the [distribution] contract, at which point Escape removed

---

party's proposed material facts in a summary judgment motion admitted where the opposing party failed to cite adequately its responsive proposed facts). Nevertheless, much of the key evidence cited throughout EMI's statement of material facts is interrelated and supportive of multiple proposed facts, thus making an assessment of the evidence as a whole more reasonable here than in a case where, for example, the court must "sift through a large court record [on] the possibility that it will find something . . . that the . . . party has not bothered to call to its attention." Morisseau v. DLA Piper, 532 F. Supp. 2d 595, 618 (S.D.N.Y. 2008).

EMI's fingerprints from its filter." (SMF ¶ 75.) To support this fact, EMI cites only to a portion of the Fuquen deposition from this action. (Id.; Semel Decl., Ex. 3 at 70:11-77:19.) Fuquen, however, does not discuss blocked content in the cited portion of his deposition, and, in fact, immediately preceding the cited portion, Fuquen specifically says that fingerprinting was not part of the process for blocking content. (Id. at 70:4-21.) Fuquen testified that Escape generated fingerprints for all its content and "matched" those fingerprints against EMI content – that is, he only discussed fingerprinting in the context of "matching," which could have been done for multiple reasons; he did not discuss fingerprinting in the context of blocking or filtering. Further, Fuquen provided ambiguous testimony as to whether Escape ever stopped fingerprint-matching EMI content: When asked if Escape had at some point stopped matching the fingerprints against EMI content, Fuquen responded, "I believe so. I don't recall exactly. I'm not sure." (Id. at 77:16-19.) Although this fact is not supported directly by EMI's cited evidence, the Court finds the fact to be established and uncontroverted for the following reasons.

First, the submitted evidence establishes that Escape did, but does not now, block content matching the fingerprints of EMI content. (See Hostert Decl. ¶ 10 (". . . Escape did engage in fingerprint filtering for EMI in connection with the license agreement between the parties[,]" but now does so only for "a small label with which Escape has an ongoing agreement"); Counter SMF ¶¶ 72, 75.) The evidence thus clarifies Fuquen's testimony regarding "matching" the fingerprints for EMI content, establishing that this matching was done to block user-submitted EMI recordings as required by the Distribution Agreement. Second, the evidence establishes that Escape stopped blocking content matching the fingerprints of EMI content upon the termination of the Distribution Agreement. (Counter SMF ¶ 75 (claiming that Escape "lost the capability of fingerprint filtering [EMI's] content" upon the termination of the Distribution

Agreement); id. ¶ 72; SMF ¶ 146.) Therefore, EMI's proposed fact at paragraph 75 of its SMF is supported adequately by the submitted evidence.

Escape purports to dispute EMI's proposed fact, but fails to do so adequately. Escape responds, "Disputed, and in so responding, Escape avers that upon plaintiff's termination of the Distribution Agreement, Escape deleted plaintiff's content from the Grooveshark library, and concomitantly, lost the capability of fingerprint filtering plaintiff's content." (Counter SMF ¶ 75.) Escape does not provide evidence sufficient to controvert EMI's proposed fact or to support the facts it proposes in response. Regarding Escape's purported deletion of and subsequent inability to filter out EMI content, Escape claims (1) to have "lost the capability of fingerprint filtering [EMI's] content" (id.); (2) to possess "fingerprint filtering capability only with respect to content owned by one record label," which is not EMI (id. ¶ 72; Hostert Decl. ¶ 10); (3) that EMI "has not provided Escape with data sufficient to permit fingerprint filtering of [EMI's] content on Grooveshark" (Counter SMF ¶ 72); and (4) that "Escape deleted . . . all audio files and related materials delivered by EMI to Escape under the Distribution Agreement" (Tarantino Decl. ¶ 32). Contradicting these assertions, Escape concedes that it has in fact retained in its database the fingerprints and metadata for the EMI content it had licensed. (Counter SMF ¶¶ 73, 74.) Further, approximately two months after the termination of the Distribution Agreement, Escape represented that it had retained the EMI fingerprints and metadata specifically to preserve its capability to "undertake certain types of filtering of EMI content on the Grooveshark website." (Semel Decl., Ex. 19 (May 10, 2012 email from Escape's counsel, Matthew Giger).) Escape has therefore not shown that it ever lost the capability to filter out content matching the fingerprints and metadata of EMI content. At most, Escape's evidence shows that there may be a question as to whether Escape has the ability to filter EMI content that been added to the EMI

catalogue or that has somehow changed since its associated data was provided to Escape under the Distribution Agreement.

IV. Whether EMI Is Entitled to Judgment as a Matter of Law

Based on the facts the Court finds uncontroverted and established by the submitted evidence, the Court must determine whether EMI is entitled to judgment as a matter of law. EMI moves for summary judgment, first, on its claim against Escape for direct infringement of EMI's pre- and post-1972 recordings, including direct infringement of EMI's right of public performance and right of reproduction. Second, EMI moves for summary judgment on its claim against Escape for secondary infringement, including on theories of vicarious liability and contributory liability with respect to Grooveshark users' direct infringement. Finally, EMI moves for summary judgment on Escape's affirmative defense of safe harbor under the DMCA.

In opposition to EMI's claims for direct and secondary infringement, Escape's arguments are based only on its evidentiary objections, which, as discussed, should be overruled, and Escape's assertion that EMI released Escape for any claims with respect to "uploads" that occurred before EMI terminated the Distribution Agreement on March 22, 2012. This assertion is unavailing – the undisputed evidence establishes that EMI released Escape as to claims for infringement that accrued before or on December 31, 2010 only, and there is no evidence that Escape was ever released from all claims "arising from . . . uploads" that occurred during a given period. (Opp'n at 12-13.) Therefore, with respect to EMI's claims, Escape does not offer any argument supported by facts as to whether EMI has met its evidentiary burden. Escape's opposition thus turns on its argument that EMI has failed to demonstrate that no reasonable jury could find Escape immune from monetary liability under the DMCA's safe harbor provision.

A. Direct Infringement

The Copyright Act confers upon copyright owners "the exclusive rights to do and to authorize" various things regarding the copyrighted work. 17 U.S.C. § 106. "To establish a claim of [direct] copyright infringement, a plaintiff must establish (1) ownership of a valid copyright and (2) unauthorized copying or a violation of one of the other exclusive rights afforded copyright owners pursuant to the Copyright Act." Arista Records LLC v. Usenet.com, Inc., 633 F. Supp. 2d 124, 146 (S.D.N.Y. 2009) (internal quotation marks omitted); see also ABC v. Aereo, Inc., 874 F. Supp. 2d 373, 381-382 (S.D.N.Y. 2012), aff'd, WNET v. Aereo, Inc., 712 F.3d 676 (2d Cir. 2013), cert. granted 134 S. Ct. 896, 2014 WL 92369 (2014). EMI has established that it owns or has the exclusive right in the United States to enforce copyrights in 2,807 sound recordings, thus satisfying the first prong. With respect to the second prong, EMI alleges that Escape violates its right of public performance and its right of reproduction in its copyrighted works, as discussed below.

1. Right of Public Performance

A copyright owner has the exclusive right, "in the case of sound recordings, to perform the copyrighted work publicly by means of a digital audio transmission." 17 U.S.C. § 106(6). The Court of Appeals has found that "'to perform' a musical work entails contemporaneous perceptibility," meaning that a recording is performed when it is actually played for a listener, as opposed to when "a recording . . . is simply delivered to a potential listener." United States v. Am. Soc. of Composers, Authors, Publishers, 627 F.3d 64, 72-73 (2d Cir. 2010); see also Cartoon Network LP, LLLP v. CSC Holdings, Inc. ("Cartoon Network"), 536 F.3d 121, 134 (2d Cir. 2008) ("[A] transmission of a performance is itself a performance."). Generally, a digital transmission is "public" under the Copyright Act if the source of that transmission (e.g., the MP3

file) is capable of producing transmissions that are "received by the public," rather than producing transmissions that are potentially received by "only one subscriber." Aereo, 712 F.3d at 689. Thus, generally, a transmission is not public where a unique copy of a recording is created for each listener who wishes to play the recording, making each transmission available only to the single subscriber for whom that unique copy was made. Id. at 689-90. Files streamed over the internet are typically public under this definition, and the Court of Appeals has found "internet streaming" to "produce[] public performances." Aereo, 712 F.3d at 692; see also Capitol Records, LLC v. ReDigi Inc., 934 F. Supp. 2d 640, 652 (S.D.N.Y. 2013) (finding "audio streams" to be public performances).

By streaming a song on Grooveshark.com, a user is only able to listen to the song contemporaneously with the stream; a user cannot receive delivery of the file of the recording. This constitutes a performance under the Copyright Act. And that performance is public under the Copyright Act because Grooveshark streams content to users by storing a single master copy of each recording in its central library and allowing multiple users to share access to that same file; no unique files capable of transmission to only one subscriber are created. Between March 23, 2012, and October 2013, Grooveshark streamed EMI's copyrighted recordings, without authorization, to its users over 12 million times. Therefore, EMI has presented evidence sufficient to show that it is entitled to summary judgment on its claim for direct infringement of its right to public performance of its copyrighted audio recordings.

2. Right of Reproduction

A copyright owner has the exclusive right to "reproduce the copyrighted work in copies." 17 U.S.C. § 106(1). Under the Copyright Act, "copies" are defined as "material objects, other than phonorecords, in which a work is fixed by any method now known or later developed, and

from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device." 17 U.S.C.A. § 101. The Court of Appeals has found that the Copyright Act "imposes two distinct but related requirements: the work must be embodied in a medium, i.e., placed in a medium such that it can be perceived, reproduced, etc., from that medium (the 'embodiment requirement'), and it must remain thus embodied 'for a period of more than transitory duration' (the 'duration requirement')." Cartoon Network, 536 F.3d at 127 (quoting 17 U.S.C. § 101).

EMI provides no legal support for its claim that Escape violated its right of reproduction in its copyrighted works. EMI contends that "[t]he process by which users submit files to Escape's servers makes it clear that Escape itself can be held responsible for such reproductions." (Mot. at 8.) Because Escape has discretion over whether user-submitted content is uploaded to Grooveshark and makes "the decision whether to copy," EMI argues, "Escape can be held directly responsible for the copy that occurs during uploads." (Id.) As discussed regarding paragraph 54 of EMI's SMF, there is no factual support for EMI's assertion that Escape makes any copies. And there is no legal support for EMI's contention that unauthorized copying by Grooveshark users would result in Escape's liability for direct infringement. Indeed, the Copyright Act allows for secondary liability to address these exact types of factual allegations. See Arista Records LLC v. Doe 3, 604 F.3d 110, 118 (2d Cir. 2010) (stating that "contributory infringement liability . . . exists if the defendant engaged in personal conduct that encourages or assists the infringement") (internal quotation marks and citations omitted). EMI's arguments and evidence are premised squarely in secondary liability theory and are insufficient to show that Escape is liable for direct infringement of EMI's right of reproduction.

The Court notes that EMI's reproduction rights claim refers only to alleged copying "that occurs during uploads." (Mot. at 8.) EMI's argument does not address the unsettled area of law regarding the copying that is inherent in the digital streaming process. See John Kennedy, et al., *Performance by Means of Digital Audio Transmission*, 1 Internet Law and Practice § 12:14 (2013) ("Digital audio streams are transmitted in packets . . . [that] are temporarily stored in [a computer's memory] as 'buffer' copies until they are delivered."). Because EMI does, however, establish facts regarding Escape's lack of authorization "to copy or stream" EMI content, the Court considers EMI's facts with respect to the relationship between digital streaming and rights of reproduction. (See SMF ¶¶ 8, 26.)

In Cartoon Network, the Court of Appeals addressed the issue of whether the defendant, Cablevision Systems Corporation ("Cablevision"), infringed the reproduction rights of copyright owners through its Digital Video Recording ("DVR") streaming system. Specifically, the court assessed whether the DVR's process of saving the recording to a computer memory "buffer," and then playing the recording to the viewer from the buffer on demand, constituted reproduction of the work in copies. Cartoon Network, 536 F.3d at 127-133. The court stated that, unless the embodiment requirement and the duration requirement "are met, the work is not 'fixed' in the buffer, and, as a result, the buffer data is not a 'copy' of the original work whose data is buffered." Id. at 127. The court found that Cablevision did not infringe the copyright owners' reproduction rights because each bit of data stayed in the DVR buffer for 1.2 seconds only and was then overwritten as soon as it was processed, "strongly suggest[ing] that the works in this case are embodied in the buffer for only a 'transitory' period, thus failing the duration requirement." Id. at 130. The court thus engaged in a fact-specific inquiry, distinguishing the 1.2 seconds that the data stayed in the computer's memory from cases in which "the data . . .

remained embodied in the computer's RAM memory until the user turned the computer off." Id. at 129-30. The court also distinguished between "standard set-top DVR[s]," through which the viewer "send[s] signals from the remote to an on-set box," and the on-demand video streaming service at issue, through which "the viewer sends signals from the remote, through the cable, to . . . Cablevision's central facility," where the buffering occurs. Id. at 125.

There is no submitted evidence that would allow the Court to reach any conclusions as to whether the process by which Grooveshark streams MP3 files results in unauthorized reproduction – i.e., evidence bearing on whether the streaming process creates copies of the copyrighted work that are long enough or complete enough for the copy to be considered "fixed" under the Copyright Act. Therefore, EMI's evidence does not establish that Escape reproduces EMI's copyrighted work "in copies," 17 U.S.C. § 106(1), either through the uploading process or through the streaming process. EMI's motion for summary judgment should thus be denied as to its right of reproduction claim.

B. Secondary Infringement

"Secondary liability for copyright infringement may be imposed on a party that has not directly infringed a copyright, but has played a significant role in direct infringement committed by others, for example by providing direct infringers with a product that enables infringement." Lime Group, 784 F. Supp. 2d at 422-23 (citing Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 929-30 (2005)). EMI argues that Escape is secondarily liable for the direct infringement by Grooveshark users under theories of both vicarious and contributory liability.

1. Direct Infringement by Grooveshark Users

"To recover on a claim based on secondary liability, a plaintiff first must establish direct infringement by the relevant third party, *i.e.* the party that received the infringement-enabling

device." Id. at 423. EMI has established that it owns or has the exclusive right in the United States to enforce copyrights in 2,807 sound recordings. Between March 23, 2012, and October 2013, Grooveshark users, without authorization, submitted to Escape's servers 13,855 distinct files containing recordings of EMI's copyrighted works. By making unauthorized copies and publicly sharing them through Grooveshark.com, Grooveshark users directly infringed EMI's rights of reproduction and distribution under the Copyright Act. See id. at 423-24; A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1014 (9th Cir. 2001); Capitol Records, Inc. v. MP3tunes, LLC, 821 F. Supp. 2d 627, 647 (S.D.N.Y. 2011), reconsideration granted on other grounds, 2013 WL 1987225 (S.D.N.Y. May 14, 2013).

2. Vicarious Liability

"The common law imposes liability for vicarious copyright infringement '[w]hen the right and ability to supervise coalesce with an obvious and direct financial interest in the exploitation of copyrighted materials—even in the absence of actual knowledge that the copyright [work] is being impaired.'" Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 36 (2d Cir. 2012) (quoting Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2d 304, 307 (2d Cir. 1963)); cf. id. at 36-38 (finding that, though the language for common law vicarious liability and DMCA safe harbor is similar, they are distinct inquiries). "A defendant is liable for vicarious copyright infringement by 'profiting from direct infringement while declining to exercise a right to stop or limit it.'" Usenet.com, 633 F. Supp. 2d at 156 (quoting Grokster, 545 U.S. at 930). Thus, to be vicariously liable for Grooveshark users' direct infringement, Escape "must have (1) had the right and ability to supervise the infringing conduct and (2) received a financial benefit directly attributable to the infringing conduct." Capitol Records, Inc. v. MP3tunes, LLC, 07 Civ. 9931 (WHP), 2013 WL 1987225, at *9 (S.D.N.Y. May 14, 2013) (citing Usenet.com, 633 F.

Supp. 2d at 156). "Under the common law vicarious liability standard, there must be 'a causal relationship between the infringing activity and any financial benefit a defendant reaps, regardless of how substantial the benefit is in proportion to a defendant's overall profits.'" Id. (quoting Ellison v. Robertson, 357 F.3d 1072, 1079 (9th Cir. 2004)).

a. The Right and Ability to Supervise the Infringing Conduct

The Court of Appeals for "the Second Circuit has found that a defendant need not have 'formal power to control' where a direct infringer 'depend[s] upon [the defendant] for direction.'" Usenet.com, 633 F. Supp. 2d at 157 (quoting Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971)). "Rather, '[t]he ability to block infringers' access to a particular environment for any reason whatsoever is evidence of the right and ability to supervise.'" Id. (quoting Napster, 239 F.3d at 1023).

The undisputed evidence establishes that Escape has the right and ability to supervise Grooveshark users' infringing conduct, but does not exercise that right to stop infringement. Escape reserves the express right to control users' activity on Grooveshark. Users commit infringement by submitting files to be uploaded to Grooveshark's library, which users can only do by registering a Grooveshark account. To register an account, users must agree to Escape's Terms of Service, which permit Escape to, among other things, terminate accounts, revoke privileges, and remove user-submitted content at its discretion. Like in Arista Records LLC v. Lime Group, Escape has "the right and ability to limit the use of its product for infringing purposes, including by (1) implementing filtering; (2) denying access; and (3) supervising and regulating users." Lime Group, 784 F. Supp. 2d at 435. Escape is able to filter user-submitted content and currently does so for works owned by one small label with which Escape has an agreement. Escape can deny access by either terminating a user's account or disabling a user's

uploading capability. Escape is able to supervise and regulate users by processing their file submissions through different filters and databases, which it currently does for purposes other than to curtail infringement. Finally, Escape "controls the means of infringement . . . by hosting the infringing materials on its own servers." Disney Enters., Inc. v. Hotfile Corp., 11 Civ. 20427 (KMW), 2013 WL 6336286, at *4 (S.D. Fla. Sept. 20, 2013).

b. Direct Financial Benefit

"Under the common law vicarious liability standard, there must be 'a causal relationship between the infringing activity and any financial benefit a defendant reaps, regardless of how substantial the benefit is in proportion to a defendant's overall profits.'" MP3tunes, 2013 WL 1987225, at *9 (quoting Ellison, 357 F.3d at 1079). This causal relationship is established when the service provider "profit[s] from its ability to attract infringing users, including through increased advertising revenue." Lime Group, 784 F. Supp. 2d at 435. "[T]he law is clear that to constitute a direct financial benefit, the 'draw' of infringement need not be the primary, or even a significant, draw—rather, it need only be 'a' draw. Usenet.com, 633 F. Supp. 2d at 157. Additionally, evidence of financial gain is not necessary to prove vicarious liability as long as the service provider has an economic incentive to tolerate infringing conduct. See MP3tunes, 2013 WL 1987225, at *10.

Here, infringing content is a substantial draw to Grooveshark.com, as demonstrated by the fact that approximately 84.5% of the website's streams are of works belonging to major labels with whom Escape has no license. Approximately 80% of Escape's revenue is derived from website advertisements, and the more visitors Grooveshark attracts, the more advertising revenue Escape will earn. Escape thus has a clear economic incentive to tolerate the infringing users who supply Grooveshark with its music content, as demonstrated by Grooveshark's

promotional materials, which emphasize its large number of visitors and its music library, promoted as "the largest of any streaming service." (Semel Decl., Ex. 12.)

The undisputed facts establish that Escape receives a direct financial benefit from copyright infringement (including the infringement of EMI's content) and that Escape declines to exercise its right and ability to control or limit infringement on their servers. Accordingly, EMI's motion for summary judgment should be granted as to its claim for vicarious copyright infringement.

3. Contributory Liability

"A defendant may be held liable for contributory copyright infringement if, 'with knowledge of the infringing activity,' it 'materially contributes to the infringing conduct of another.'" Lime Group, 784 F. Supp. 2d at 432 (quoting Matthew Bender & Co., Inc. v. West Pub. Co., 158 F.3d 693, 706 (2d Cir. 1998). To show "material contribution," a plaintiff must establish "that the defendant (1) had actual or constructive knowledge of the infringing activity, and (2) encouraged or assisted others' infringement, or provided machinery or goods that facilitated infringement." Id.

First, the evidence demonstrates that Escape had knowledge of the infringing activity, as shown through Escape's own projections as to its streaming of unlicensed content and the DMCA takedown notices of infringement it received. Further, Tarantino acknowledged that "the great majority of content" on Grooveshark at one point came "from illegal networks," and Escape's co-founders, Tarantino and Greenberg, were each recorded for infringement of 105 works and 687 works, respectively.

Second, the evidence establishes that Escape materially contributed to its users' infringement by providing the "site and facilities or the environment and market for infringing

activity." Usenet.com, 633 F. Supp. 2d at 155 (internal quotation marks omitted). Escape provided all the mechanisms to allow for infringing activity, including the servers to host and the software to submit the infringing content, the tools for organizing the submitted files and facilitating their access and searchability, and the interface for users to select and stream infringing content to their devices.

Escape offers no defenses to EMI's contributory infringement claim. The evidence establishes that Escape had knowledge of its users' infringing activity and materially contributed to it. Accordingly, EMI's motion for summary judgment should be granted on its claim for contributory infringement.

C. Common Law Copyright Infringement

Under the Copyright Act, "sound recordings first fixed before February 15, 1972" are governed by state "common law or statute," not by federal law. See 17 U.S.C. § 301(c); Lime Group, 784 F. Supp. 2d at 436. "[T]he elements for a direct infringement claim under federal law mirror those for infringement of common law copyright under [New York] state law." ReDigi, 934 F. Supp. 2d at 657 (citing Capitol Records, Inc. v. Naxos of Am., Inc., 4 N.Y.3d 540, 563 (2005)). Thus, the Court's findings that EMI is entitled to summary judgment on its direct infringement claims under the Copyright Act, except with respect to its right of reproduction claim, also apply under the common law for EMI's pre-1972 recordings.

Courts in this district have also recognized that claims for secondary liability are available under state common law. See Lime Group, 784 F. Supp. 2d at 436 (quoting Grokster, 545 U.S. at 930, 934-36) ("[S]econdary liability for infringement, including claims for . . . contributory and vicarious infringement, 'emerged from common law principles.'") (citing Underhill v. Schenck, 238 N.Y. 7 (1924)). While the elements of contributory and vicarious

copyright infringement under New York common law are not explicitly delineated, the case law indicates that theories of secondary liability generally mirror federal law. See id. (finding that the secondary liability theory of inducement of infringement under the common law mirrors federal law); James v. Universal Motown Records, Inc., 03 Civ. 4487 (LAK), 2004 WL 2847852, at *1 (S.D.N.Y. Dec. 10, 2004) (recognizing that common law claims for contributory copyright infringement of works fixed after 1972 are preempted by federal claims of contributory infringement under the Copyright Act). Escape does not argue that it is not liable for common law copyright infringement as to EMI's pre-1972 works, except to assert its DMCA safe harbor defense. Applying the same analysis as required under the Copyright Act to EMI's common law copyright secondary infringement claims for its works fixed before February 15, 1972, the Court recommends granting summary judgment in favor of EMI.

D. Whether Escape is Ineligible for DMCA Safe Harbor as a Matter of Law

1. DMCA Safe Harbor

The DMCA was enacted in 1998 "to 'clarif[y] the liability faced by service providers who transmit potentially infringing material over their networks,'" YouTube, 676 F.3d at 26-27 (quoting S. Rep. No. 105–190 at 2 (1998)), and to "balance the interests of copyright owners and online service providers by promoting cooperation [and] minimizing copyright infringement," MP3tunes, 821 F. Supp. 2d at 636. "To that end, [the DMCA] established a series of four 'safe harbors' that allow qualifying service providers to limit their liability for claims of copyright infringement based on (a) 'transitory digital network communications,' (b) 'system caching,' (c) 'information residing on systems or networks at [the] direction of users,' and (d) 'information location tools.'" YouTube, 676 F.3d at 27 (quoting 17 U.S.C. § 512(a)-(d)).

As a prerequisite to eligibility for any of the four safe harbor categories, a defendant must first establish that it satisfies certain criteria, including, as relevant here, demonstrating "the adoption and reasonable implementation of a 'repeat infringer' policy that 'provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network.'" YouTube, 676 F.3d at 27 (quoting 17 U.S.C. § 512(i)(1)(A)). If the defendant establishes that it meets the threshold criteria of § 512(i), the defendant must then show that it satisfies the requirements of a particular safe harbor category. Id. Here, Escape seeks protection under § 512(c), "which covers infringement claims that arise 'by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider.'" Id. (quoting 17 U.S.C. § 512(c)(1)).

Safe harbor is an affirmative defense and thus imposes on the defendant "'the burden of establishing that he meets the statutory requirements.'" Capitol Records, LLC v. Vimeo, LLC, 09 Civ. 10101 (RA), 2013 WL 5272932, at *6 (S.D.N.Y. Sept. 18, 2013) (quoting Columbia Pictures Indus., Inc. v. Fung, 710 F.3d 1020, 1039 (9th Cir. 2013)). "[A] finding of safe harbor application necessarily protects a defendant from all affirmative claims for monetary relief." YouTube, 676 F.3d at 41 (citing 17 U.S.C. § 512(c)(1)). "As courts have emphasized, '[t]his immunity . . . is not presumptive, but granted only to 'innocent' service providers'" and should be "narrowly construed." MP3tunes, 821 F. Supp. 2d at 636 (quoting ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619, 625 (4th Cir. 2001)).

EMI argues that Escape is ineligible for DMCA safe harbor for several reasons, including that Escape cannot satisfy the "repeat infringer policy" prerequisite under § 512(i)(1)(A). Because Escape cannot assert any safe harbor defense if it does not meet this requirement, the

Court first addresses whether EMI is entitled to judgment as a matter of law based on its assertion that Escape fails the "repeat infringer policy" element of the DMCA.

2. Repeat Infringer Policy

a. Legal Standard

To be eligible for immunity from monetary relief under any of the DMCA's four safe harbor categories, a service provider must demonstrate that it "has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers[.]" 17 U.S.C. § 512(i)(1)(A). This repeat infringer policy requirement "is a fundamental safeguard for copyright owners" and "essential to 'maintain the strong incentives for service providers to prevent their services from becoming safe havens or conduits for known repeat copyright infringers.'" MP3tunes, 821 F. Supp. 2d at 637 (quoting Perfect 10 v. Cybernet Ventures, 213 F. Supp. 2d 1146, 1178 (C.D. Cal. 2002)). "The purpose of subsection 512(i) is to deny protection to websites that tolerate users who flagrantly disrespect copyrights." Id.

"To fulfill the requirements of 17 U.S.C. § 512(i), a service provider must (i) adopt a policy that provides for the termination of service access for repeat copyright infringers; (ii) inform users of the service policy; and (iii) implement the policy in a reasonable manner." Wolk v. Kodak Imaging Network, Inc., 840 F. Supp. 2d 724, 744 (S.D.N.Y. 2012); see also Hotfile, 2013 WL 6336286, at *8 ("Under the DMCA, Internet service providers must reasonably implement a policy designed to terminate users identified as repeat infringers."). Section 512(i)'s key terms – "reasonably implemented" and "repeat infringer" – are not defined in the DMCA. See MP3tunes, 821 F. Supp. 2d at 637. Courts have found that "a reasonably implemented

[repeat infringer] policy can utilize a 'variety of procedures[.]'" Vimeo, 2013 WL 5272932, at *10 (quoting Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1109-11 (9th Cir. 2007)). Factors that have been applied to determine whether a repeat infringer policy is reasonably implemented include whether the service provider "(1) has a system for responding to takedown notices, (2) does not interfere with the copyright owners' ability to issue notices, and (3) under 'appropriate circumstances' terminates users who repeatedly or blatantly infringe copyrights." MP3tunes, 821 F. Supp. 2d at 637 (citing CCBill, 488 F.3d at 1109-10). In addition, "service providers that purposefully fail to keep adequate records of the identity and activities of their users and fail to terminate users despite their persistent and flagrant infringement are not eligible for protection under the safe harbor." Id. Although a service provider "must do what it can reasonably be asked to do to prevent use of its service by 'repeat infringers,'" In re Aimster Copyright Litig., 334 F.3d 643, 655 (7th Cir. 2003), the DMCA does not impose an affirmative duty on a service provider to "police its users," Vimeo, 2013 WL 5272932, at *10 (internal quotation marks omitted).

b. Adoption of a Policy

EMI must first show that Escape has not adopted a policy of terminating repeat infringers' access to Grooveshark in appropriate circumstances. "This statutory requirement emanates from Congress' concern that 'those who repeatedly or flagrantly abuse their access to the Internet through disrespect for the intellectual property rights of others should know that there is a realistic threat of losing that access.'" Vimeo, 2013 WL 5272932, at *9 (quoting H.R. Rep. 105-551 pt. 2, at 61 (1998)). "[T]he threshold requirement of the adoption of a repeat infringer policy should not be an overly burdensome one to meet." Id.

The evidence establishes that Escape has adopted a formal policy providing for the termination of repeat infringers' access to Grooveshark. Grooveshark's Terms of Service requires account-holders to agree that they are not submitting infringing content, and specifically states that if Grooveshark finds an account-holder to be a "repeat infringer," it will "terminate [the user's] account and delete all data associated with [the] account." (Semel Decl., Ex. 14.) Additionally, Escape maintains a "one strike policy," which provides for the disabling of uploading capabilities for an account-holder after Escape receives one DMCA takedown notification regarding a file uploaded by that account-holder. On similar evidence, the court in Capitol Records v. Vimeo found that the service provider, Vimeo, demonstrated that it had adopted a sufficient policy, stating that, "[a]t this stage of the analysis, it appears sufficient that Vimeo demonstrate that it took a clear position that those who chose to violate another's copyright would not be permitted to avail themselves of the service Vimeo provides." Vimeo, 2013 WL 5272932, at *9. In light of the language in Escape's Terms of Service and the evidence demonstrating Escape's one strike policy, the Court finds that Escape has likewise met the minimum requirement for adoption of a formal policy that provides for the termination of service access for repeat infringers.

c. Informing Users of the Service Policy

The DMCA requires "that the service provider 'put users on notice that they face exclusion from the service if they repeatedly violate copyright laws.'" Id. at *10 (quoting Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1102 (W.D. Wash. 2004), overruled on other grounds Cosmetic Ideas, Inc. v. IAC, 606 F.3d 612 (9th Cir. 2010)). In addition to the language in the Terms of Service, Grooveshark users must click a box before uploading files agreeing that they understand the Terms of Service and are "only uploading content that does not infringe

upon the rights of others." Given the explicit notice to users in the Terms of Service and the implicit notice that appears on the screen before a user can submit content, the Court finds that Escape satisfies the requirement to inform Grooveshark that they may be subject to Escape's repeat infringer policy.

d. Reasonable Implementation of the Policy

Whether the repeat infringer policy is "reasonably implemented" is the threshold issue under § 512(i)(1)(A) that has been most analyzed by the courts and is most salient to EMI's motion for summary judgment on Escape's safe harbor defense. In light of Congress's decision to leave the "'obligations of service providers[] loosely defined,'" courts have approached the inquiry into reasonable implementation in different ways. Vimeo, 2013 WL 5272932, at *9 (quoting Amazon.com, 351 F. Supp. 2d at 1101). Given the nature of the material facts at issue here, it is useful to proceed by assessing "reasonable implementation" as two distinct elements – first analyzing whether Escape actually "implemented" its policy, and, if it did, then analyzing whether the implementation was reasonable, i.e., implemented "in appropriate circumstances." 17 U.S.C. § 512(i)(1)(A). Accord CCBill, 488 F.3d at 1110-15 (analyzing "implementation" and "reasonableness" separately).

i. Whether Escape Implemented Its Policy

This inquiry focuses on whether Escape actually implements or would be capable of implementing, in any circumstance, the repeat infringer policy that it has adopted. "Adopting a repeat infringer policy and then purposely eviscerating any hope that such a policy could ever be carried out is not an 'implementation' as required by § 512(i)." In re Aimster Copyright Litig., 252 F. Supp. 2d 634, 659 (N.D. Ill. 2002), aff'd, 334 F.3d 643 (7th Cir. 2003). While there is little guidance in the DMCA or the relevant case law as to when a repeat infringer policy is

"implemented," the cases that do exist have examined the following issues that the Court finds probative to this matter: whether the service provider actively prevented copyright owners from collecting information necessary to issue effective DMCA takedown notifications, see CCBill, 488 F.3d at 1109-10; Vimeo, 2013 WL 5272932, at *12; and whether implementation would result in the "termination" of repeat infringers, see Myxer, 2011 WL 11660773, at *16-18; Veoh, 665 F. Supp. 2d at 1118. The Court examines these issues by looking to the facts regarding Escape's record-keeping practices as to repeat infringers, its organization of user-submitted files on Grooveshark.com, and the actions Escape takes or purports to take against account-holders who submit allegedly infringing files.

To clarify the subject of this discussion at the outset, it is undisputed that Escape does not implement the repeat infringer policy stated in its Terms of Service and that the Court found Escape to have formally adopted. Under the Terms of Service policy, if a user (referred to as "you" in the Terms of Service) continues to upload infringing content after Escape has taken action to disable the user's uploading ability, "you will be considered a repeat infringer, and [Escape] will terminate your account and delete all data associated with your account; remove all the User Content you have uploaded/submitted to the Site; and use its reasonable efforts to prohibit you from signing up for another User account in the future." (Semel Decl., Ex. 14 at 4.) Escape does not contend that this is actually its policy, has never taken any of these actions against a user, and does not have any procedures for taking these actions against a user. Thus, the relevant repeat infringer policy for this discussion is what Escape refers to as its one strike policy.

1. Record Keeping

A service provider's failure to maintain adequate records of infringement and of users committing infringement may prevent implementation of a repeat infringer policy, thus disqualifying the service provider from safe harbor under the DMCA. See MP3tunes, 821 F. Supp. 2d at 637 ("[S]ervice providers that purposefully fail to keep adequate records of the identity and activities of their users and fail to terminate [repeat infringers] . . . are not eligible for protection under the safe harbor."); CCBill, 488 F.3d at 1110 (discussing whether the defendants "prevented the implementation of their policies by failing to keep track of repeatedly infringing webmasters" and stating that "a substantial failure to record webmasters associated with allegedly infringing websites may" preclude a service provider from establishing on summary judgment that it implemented its repeat infringer policy).

EMI argues that Escape's record-keeping practices prevented Escape from implementing its repeat infringer policy. The submitted evidence establishes that (1) Escape does not record users who receive multiple DMCA takedown notices; (2) Escape, in response to a DMCA takedown for an infringing song, does not record users who submitted or who later submit the infringing song other than the one user who submitted the primary file; (3) Escape does not record any users who submitted files that are taken down under Escape's DMCA Lite procedure; (4) in one of the database tables in which Escape logs DMCA takedowns, 94.2% of the takedown entries are recorded in the "dmca_lite" field, as opposed to the "dmca" field; and (5) one of the database tables in which Escape logs DMCA takedowns contains no entries from October 31, 2010 through March 20, 2012.

Escape argues that these facts are irrelevant because, under its one strike policy, which requires disabling uploading capability for any user who receives even one notice of

infringement under the DMCA, "it's not possible for [the infringer] to repeat" her infringing activity. (Semel Decl., Ex. 1 (Hostert Dep. at 137:13-20).) Thus, because "there can't be repeat infringers," keeping the type of records cited by EMI would be superfluous. (Id. at 137:23-25.) According to Escape, "[t]his *one-time* infringer policy is *more* than is required by the DMCA." (Opp'n at 35.)

Escape's argument fails for several reasons.[18] First, even if Escape's one strike policy were entirely effective, the claim that this policy is "more" than the DMCA requires is misleading. That is, a largely effective one strike policy may be "more" than is required in the sense that it would be *different* than what is required, while still producing results sufficient to satisfy the DCMA requirement. It is a dubious proposition, however, that a one strike policy would be "more" than is required in the sense that it would *better* effect the principles and goals of the DMCA than would a more literal policy of terminating the accounts of users who have repeatedly committed acts of copyright infringement. Congress enacted the DMCA "to update copyright law for the digital age," YouTube, 676 F.3d at 26, "recogniz[ing] that '[i]n the ordinary course of their operations, service providers must engage in all kinds of acts that expose them to potential copyright infringement liability,'" Vimeo, 2013 WL 5272932, at *5 (quoting S. Rep. No. 105-190, at 8 (1998)). For websites that allow users to share digital content, some degree of copyright-infringing activity is all but inevitable. Cf. Aimster, 334 F.3d at 655 (stating that the "DMCA is an attempt to deal with special problems created by the so-called digital revolution," including "the vulnerability of Internet service providers . . . to liability for copyright infringement as a result of file swapping among their subscribers"). Indeed, the Supreme Court has recognized that, [w]hen a widely shared service . . . is used to commit

[18] The Court's conclusions in this section regarding the adequacy of Escape's record-keeping policy and practice assume that the action Escape purports to take against infringing users does constitute "termination" under the DMCA, a proposition discussed below.

infringement, it may be impossible to enforce rights in the protected work effectively against all direct infringers." Grokster, 545 U.S. at 929-30 (also noting the "the number of infringing downloads that occur every day using [the defendants' file-sharing] software"); see also Universal City Studios, Inc. v. Corley, 273 F.3d 429, 435 (2d Cir. 2001) (stating that, in enacting the DMCA, Congress was mindful that "the ease with which pirates could copy and distribute a copyrightable work in digital form was overwhelming the capacity of conventional copyright enforcement to find and enjoin unlawfully copied material").

Acknowledging this reality, Congress passed the DMCA to "limit[] the liability of service providers," thus fostering the expansion of "the variety and quality of services on the Internet" and decreasing the burden on service providers to snuff out each instance of infringement in order to make providers less likely to "hesitate to make the necessary investment in the expansion of the speed and capacity of the internet." S. Rep. No. 105-190 at 8; see also Grokster, 545 U.S. at 929 (noting the concern that too widely "imposing liability . . . could limit further development of beneficial technologies"). For this reason of practicality, the fundamental and primary responsibility of service providers under the DMCA is to prevent *repeat* infringement. See Ellison v. Robertson, 189 F. Supp. 2d 1051, 1064 (C.D. Cal. 2002) ("On its face, subsection (i) is only concerned with repeat-infringer termination policies, and not with copyright infringement in general."); MP3tunes, 821 F. Supp. 2d at 637 (quoting Aimster, 334 F.3d at 655) ("As described by Judge Posner, '[t]he common element of [the DMCA's] safe harbors is that the service provider must do what it can reasonably be asked to do to prevent the use of its service by 'repeat infringers.'"); CCBill, 488 F.3d at 1111 ("Section 512(i) itself does not clarify when it is 'appropriate' for service providers to act. It only requires that a service provider terminate users who are 'repeat infringers.'"); Hotfile, 2013 WL 6336286, at *9, *24-25

(granting plaintiff's motion for summary judgment as to defendant's DMCA defense because defendant's repeat infringer policy was "legally insufficient" where defendant had "official policies forbidding infringement" but "did not significantly address the problem of *repeat* infringement," and further noting that, under the policy, "whether a user was the subject of one notice [of infringement] or 300 notices, [defendant] acted no differently in terms of investigating possible infringement") (emphasis supplied). A policy that prioritizes targeting first-time infringers at the expense of more effectively terminating repeat infringers is not "more" than the DMCA requires in any sense that furthers the DMCA's purpose.[19] Indeed, Congress's "explicit repudiation of any affirmative duty on the part of service providers to monitor user content [for] . . . 'facts indicating infringing activity,'" MP3tunes, 2013 WL 1987225, at *2 (quoting 17 U.S.C. § 512(m)), demonstrates the DMCA's fundamental concern with terminating the accounts of user "who are *repeat* infringers," Veoh, 665 F. Supp. 2d at 1116 (emphasis in original). Therefore, even if Escape had presented evidence showing that its one strike policy effectively terminated most first-time infringers, the policy likely would be insufficient if it did not meaningfully catch repeat infringers.

Second, there is significant undisputed evidence that Escape's one strike policy does *not* prevent repeat infringement. There are 3,323 users who submitted content listed in Escape's DMCA takedowns database ("users_dmca_takedowns") who still had the ability to upload files to Grooveshark, and 1,609 users who were recorded for a DMCA takedown after having already been sent at least one DMCA notice of infringement from Escape. The evidence further reveals Grooveshark users who have been recorded for infringement in connection with over 1,000 recordings. In addition, 568 users were recorded for infringement for over 100 recordings,

[19] By contrast, for example, a policy under which the service provider "affirmatively police[d] its users for evidence of repeat infringement," would be "more" than the DMCA requires in a sense that might further the Act's goals. CCBill, 488 F.3d at 1111.

including Escape CEO Tarantino, recorded for infringing 105 works, and Escape Chief Technology Officer Greenberg, recorded for infringing 687 works. This data demonstrates that there is a substantial amount of repeat infringement despite Escape's one strike policy.

Third, the small number of repeat infringers are responsible for a vastly disproportionate amount of the content Grooveshark maintains in its active library. There are approximately 24,748,078 user accounts registered on Grooveshark.com. Escape has recorded 37,986 of these users for submitting works removed in a DMCA takedown, and, of those users, Escape has recorded 21,044 for submitting multiple works removed in DMCA takedowns. Despite being relatively few in number, recorded infringers are responsible for over 48% of all primary files (i.e., the playable content) in Grooveshark's active music library, and users recorded for submitting multiple infringing works are responsible for 35% of all primary files in Grooveshark's active music library. In other words, nearly half of all music content playable on Grooveshark.com was sourced by the 0.15% of account-holders with records of infringement. Further, the 1,609 users recorded for DMCA takedowns *after* having already received DMCA takedown notifications from Escape in connection with previously submitted files are responsible for 2,339,671 total files in Escape's active library and 1,263,394 playable primary files. Thus, on average, these 1,609 repeat infringers each submitted approximately 1,454 files that are housed in Grooveshark's active library. These facts illustrate why a one strike policy is not meaningfully "more" than a repeat infringer policy: even if Escape actively monitored over 99% of its account-holders for infringement, and even if Escape terminated the accounts of all one-time infringers within that monitored group, Escape could still be ignoring the infringers of multiple works who are responsible for over one-third of all primary files on Grooveshark.com, and the repeat infringers responsible for over 2.3 million files in Grooveshark's library.

The above facts, by themselves, may not establish that Escape fails to "implement" a repeat infringer policy under §512(i) as a matter of law. Rather, they establish that Escape's one strike policy cannot justify a failure to keep adequate records of repeat infringers. Escape does not try to identify repeat infringers and fails to keep records that would allow it to do so. Whether "service providers . . . purposefully fail to keep adequate records of the identity and activities of their users" is critical to safe harbor eligibility, MP3tunes, 821 F. Supp. 2d at 637, because "a reasonable policy must be capable of tracking infringers," Hotfile, 2013 WL 6336286, at *21. Escape's failure to do anything to identify repeat infringers is particularly egregious given that Grooveshark users who have been subject to a DMCA takedown comprise a fraction of 1% of all Grooveshark account-holders but supply Grooveshark with nearly half of its content. Cf. Hotfile, 2013 WL 6336286, at *10 (noting that infringing activity was carried out by "a discreet group of problematic users" and that, while users with records of multiple infringement comprised "less than one percent of all . . . users, they were responsible for posting . . . 44 percent of all files ever uploaded"). By taking a piecemeal approach to terminating infringers and not recording repeat infringers, Escape has effectively prevented itself from implementing a policy that can target the actual source of the infringing content on Grooveshark. Cf. Cybernet, 213 F. Supp. 2d at 1177 ("Making the entrance into the safe harbor too wide would allow service providers acting in complicity with infringers to approach copyright infringement on an image by image basis without ever targeting the source of these images."); Hotfile, 2013 WL 6336286, at *21 ("It is clear from the record that Hotfile's repeat infringer policy was not tied to notices of infringement it received from copyright owners under the DMCA. . . . Hotfile acknowledges that it made no connection between infringement notices and acts of infringement.

Hotfile explains that it did not track the notices and did not base its policy on how many notices were associated with certain users (such as by 'flagging' them).").

Finally, when Escape processes a DMCA takedown, it makes a record of infringement for the first user to submit that song file only; no record is made of the users who submit that song after the takedown or users who submitted song files that were stored as non-primary files. This lack of record keeping has egregious effects, as discussed below regarding Escape's organization of its central library.

2. Organization of User-Submitted Files

The manner in which Escape organizes its music library may "actively prevent copyright owners from collecting information needed to issue [DMCA] notifications" in a manner that would have any meaningful consequence. CCBill, 488 F.3d at 1109. Escape processes DMCA takedowns only when the copyright owner identifies the web address for the infringing song. This web address is associated with the primary file for that song. If Escape complies with the takedown, it removes the primary file. If Escape does this under its DMCA Lite policy, which the evidence indicates it does in the vast majority of circumstances, no other action is taken. If Escape removes the file under the regular DMCA takedown policy, a notification is sent to the user who submitted that file, thus creating a record of that user's infringement. In no circumstance is a non-primary file removed or the submitter of the non-primary file recorded. A content owner cannot obtain the web address for a non-primary file. When the primary file is removed, a non-primary file will replace it and become the playable primary file. If there are no non-primary files, the next time a user submits that infringing song, it will become the primary file and the user will not be recorded. If the same specific MP3 file that was removed (as

identified by its unique file hash) is later submitted, it will be uploaded to the library and the user will not be recorded.

The following example illustrates how the system described above operates in practice. EMI owns the copyright to the song Blueberry Hill by Fats Domino. After March 23, 2012, users submitted 107 MP3 files containing that recording. (Horowitz Decl., Ex. 13 at 7.) Through the process of "fuzzy matching" and the service provided by MusicBrainz, Escape is able to effectively group those 107 files together. The first of those files submitted is the primary file, and the 106 other files are the non-primary files. Because of this organization, EMI would only be capable of issuing a DMCA notification containing the web address of the primary file. Once Escape removes that file, the next non-primary file in line will replace it, and there will then be 105 non-primary files. That new primary file will be immediately searchable and playable. If Escape removes the file under its DMCA Lite policy, which one database indicates it does 94.2% of the time, the infringer who submitted the file will not be recorded or notified. Under any of Escape's policies, no record will be made for the users who submitted the 106 non-primary files or for users who subsequently submit an MP3 of Blueberry Hill by Fats Domino, including an MP3 with a file hash identical to the removed file.

Escape's organization of user-submitted files and its DMCA takedown practices would render it all but impossible for EMI to stop the unauthorized streaming of Blueberry Hill on Grooveshark. In In re Aimster Copyright Litigation, the district court held that Aimster did not satisfy the DMCA's repeat infringer policy requirement because it enabled its users to encrypt their file transfers, thus "render[ing] it impossible to ascertain which users are transferring which files." 252 F. Supp. 2d at 659. The Court of Appeals for the Seventh Circuit affirmed, finding that Aimster effectively "disabled itself from doing anything to prevent infringement." Aimster,

334 F.3d at 655; cf. CCBill, 488 F.3d at 1110-11 (citing Aimster as an example of insufficient "implementation" prior to addressing the question of "reasonable" implementation); Vimeo, 2013 WL 5272932, at *11-12 (discussing Aimster and CCBill's findings as to reasonable implementation). Here, by preventing copyright owners from ascertaining which Grooveshark users are submitting the non-primary files and from obtaining the web addresses for the non-primary files, copyright owners are inhibited severely from issuing DMCA notifications that have any meaningful consequences. And by failing to record all but a fraction of the users who submitted a song for which a file was removed in response to a DMCA takedown, Escape disables its capability to identify repeat infringers and terminate their accounts. As the district court found in Aimster, "[a]dopting a repeat infringer policy and then purposely eviscerating any hope that such a policy could ever be carried out is not an 'implementation' as required by § 512(i)." 252 F. Supp. 2d at 659. Such is the case here, albeit as a result of the confluence of several aspects of Escape's system, rather than a single dispositive fact as in Aimster.

As an additional matter, bearing in mind the purpose and principles underlying the DMCA, it is obvious that a service provider who has designed a system where it could receive 106 separate and consecutive notifications of infringement from a copyright owner for a single song and still allow that song to be searched and streamed by the public is not the "innocent service provider" contemplated by Congress as being eligible for safe harbor. MP3tunes, 821 F. Supp. 2d at 636 (internal quotation marks omitted); see also RemarQ Communities, Inc., 239 F.3d at 625 ("The DMCA's protection of an innocent service provider disappears at the moment the service provider loses its innocence, i.e., at the moment it becomes aware that a third party is using its system to infringe.").

3. "Termination"

Putting all the aforementioned problems with Escape's "implementation" aside, it is still not at all clear that Escape has a repeat infringer policy that "provides for the termination . . . of subscribers and account holders . . . who are repeat infringers." 17 U.S.C. § 512(i)(1)(A). Escape purports that its policy and practice is "to disable a user's uploading privileges following the receipt of *one* notice . . . of infringement under the DMCA associated with that account." (Opp'n at 35, 36 n.14.) If Escape had submitted documentary evidence demonstrating the application of this policy to an infringing user (which it did not), that infringing user, according to Escape, would still maintain her account and be able to "curate . . . her music 'collection' on Grooveshark by, *inter alia*, . . . adding and removing songs to and from [her] collection, and . . . creating sub-groupings of songs in the collection as 'playlists.'" (Opp'n at 37.) And, of course, the infringing user would be able to search for and stream recordings, as anyone can do without creating an account. Escape stresses that, once an account-holder's uploading capability is disabled, "[t]he remaining account privileges merely permit users to associate or disassociate their account from content that *already exists* on Grooveshark." (Id.)

Escape does not provide legal support for the proposition that the actions described above constitute "termination" under § 512(i)(1)(A). "[T]he DMCA's safe harbors, as with all immunities from liability[,] should be narrowly construed." MP3tunes, 821 F. Supp. 2d at 636 (citing United States v. Texas, 507 U.S. 529, 534 (1993)). Congress included plainly flexible language for the DMCA's repeat infringer policy prerequisite, requiring that the policy be implemented "reasonably" and in "appropriate" circumstances. Courts, however, have not construed the word "termination" with the same degree of flexibility. See, e.g., Hotfile, 2013 WL 6336286, at *21 (finding that the service provider "failed to reasonably implement [its policy] by

actually terminating users"); Cybernet, 213 F. Supp. 2d at 1179 ("Because the Court finds that there is a strong likelihood that Cybernet cannot establish that it has 'reasonably implemented' a policy directed at *terminating* repeat infringers, even in 'appropriate circumstances,' there is little likelihood that it can avail itself of section 512's safe harbors.") (emphasis in original). In fact, Congress and many courts have indicated strongly that "termination" requires more than what Escape purports to do.

First, the plain meaning of the DMCA's language is that, in implementing a repeat infringer policy, the service provider must, when appropriate, terminate, or "end," a subscriber's subscription or an account holder's account.[20] Looking to the DMCA as a whole, Congress differentiated between terminating accounts, which is required in § 512(i) and is permitted in the scope of injunctive relief under § 512(j), and "disabling [a user's] access to . . . activity claimed to be infringing," which service providers can do in good faith without incurring liability from the user under § 512(g)(1). Escape's policy "of disabling the ability of a user to upload files," (Opp'n at 37), is substantially similar to "disabling [a user's] access to . . . activity claimed to be infringing." But Congress chose not to use that language in § 512(i) while clearly aware of that option and distinction. It is thus reasonable to assume that Congress meant something different by "termination" and would have used other language, as it had elsewhere, if it intended to impose a flexible standard or to permit disabling the infringing activity while allowing the infringer's account and other privileges to remain active. Cf. Veoh, 665 F. Supp. 2d at 1112 & n.16 (distinguishing between § 512(c) of the DMCA, under which "the service provider must 'respond[ ] expeditiously to *remove, or disable access to,* the material,'" and § 512(i)(1)(A), under which the "limitations on liability apply only if a service provider has 'adopted and

[20] "Termination" is defined as "[t]he act of ending something; extinguishment." Black's Law Dictionary (9th ed. 2009).

reasonably implemented . . . a policy that provides for the *termination* . . . .'") (emphasis in Veoh). Further, courts should be particularly cautious in defining a term involving copyright protection in a way that is unsupported by congressional intent given the judiciary's policy of deferring to Congress on copyright matters. See Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 431 (1984) ("Sound policy, as well as history, supports our consistent deference to Congress when major technological innovations alter the market for copyrighted materials. Congress has the constitutional authority and the institutional ability to accommodate fully the varied permutations of competing interests that are inevitably implicated by such new technology."); ReDigi Inc., 934 F. Supp. 2d at 660 (stating that deference to Congress "often counsels for a limited interpretation of copyright protection").

Second, in using the word "termination," it is apparent that Congress intended for service providers to *disassociate* themselves fully from repeat infringers, not simply take measures to impede their infringing activity while allowing them to maintain the type of account privileges offered by Escape. The mandate for a repeat infringer policy as a prerequisite to any safe harbor under the DMCA "emanates from Congress' concern that 'those who repeatedly or flagrantly abuse their access to the Internet through disrespect for the intellectual property rights of others should know that there is a realistic threat of *losing that access*.'" Vimeo, 2013 WL 5272932, at *9 (quoting H.R. Rep. 105-551 pt. 2, at 61 (1998)) (emphasis supplied). Thus, when courts have used language other than "termination," that language has consistently indicated a total disassociation between the service provider and the repeat infringer. See id. (finding that, under Vimeo's policy, "those who chose to violate another's copyright would not be permitted to avail themselves of the service Vimeo provides"); MP3tunes, 821 F. Supp. 2d at 638 (describing the "blatant infringers that internet service providers are obligated to ban from their websites"); id. at

637 ("The purpose of subsection 512(i) is to deny protection to websites that tolerate users who flagrantly disrespect copyrights."); id. (quoting Cybernet, 213 F.Supp.2d at 1178) ("Other courts have described enforcement of this [repeat infringer policy] provision as essential to 'maintain the strong incentives for service providers to prevent their services from becoming safe havens . . . for known repeat copyright infringers."); Aimster, 334 F.3d at 655 (stating that a service provider must act to "prevent use of its service by 'repeat infringers'"); Cybernet, 213 F. Supp. 2d at 1178 ("Significantly, in its Opposition Cybernet maintains it . . . remove[s] from the Cybernet search engine and links page any website about which it has received a notice of infringement, without addressing its power to stop providing its [age verification system] service to known infringers.") (internal quotation marks omitted). Indeed, Escape may have had the same understanding of what the DMCA requires when it stated in its Terms of Service that it would "terminate [a repeat infringer's] account and delete all data associated with [the] account." (Semel Decl., Ex. 14.) Finding Escape's upload-disabling policy to constitute "termination" under § 512(i) would be unprecedented and antithetical to the principle of disassociation and revocation of access that has been expressed by Congress and many courts both in and outside of this district.

Finally, Escape's policy of disabling uploading capabilities does not address the concerns of the safe harbor provision Escape now invokes to the extent that actual extinguishment of repeat infringers' accounts would. Escape asserts its DMCA defense under § 512(c), the safe harbor intended to protect service providers who, by offering storage services for content "at the direction of a user," unintentionally house infringing works on their system or network. Congress distinguished this content from "[i]nformation that resides on the system or network operated by . . . the service provider through its own acts or decisions and not at the direction of a user,"

which is not protected under § 512(c). H.R. Rep. No. 105–551(II) at 53 (1998); see also Rock River Commc'ns, Inc. v. Universal Music Grp., Inc., 08 Civ. 635 (CAS)(AJW), 2011 WL 1598916, at *16 (C.D. Cal. Apr. 27, 2011). Additionally, "[t]he relevant case law makes clear that the § 512(c) safe harbor extends to software functions performed for the purpose of facilitating access to user-stored material." YouTube, 676 F.3d at 39. If Escape actually terminated the accounts of repeat infringers while maintaining the content submitted by those users in its library, Escape would face new challenges to its claim that its storage is at the now-terminated user's direction or intended to facilitate access to that content. Given that a Grooveshark "account holder's ability to control and curate his or her music 'collection'" is "[a]t the center of those privileges" attained by registering an account (Opp'n at 37), the "direction" that a user gives to Grooveshark may very well change after the user's account is terminated and all the privileges lost. If, on the other hand, Escape avoided such "direction of the user" issues by terminating repeat infringers' accounts *and* deleting their content, Escape's music library would likely be substantially reduced.[21] Thus, by not actually terminating repeat infringers' accounts, Escape avoids having to choose between either weakening its claim that it is storing information "at the direction of a user" or considerably constricting the range of music available on Grooveshark.

In sum, interpreting the word "termination" to not mean ending a repeat infringer's account would not only deviate from congressional intent, established case law, and prudential concerns of statutory interpretation, but would also have the inequitable result of benefiting

[21] As an illustration, Escape claims that it has "terminated the uploading privileges of nearly 39,000 user accounts[] in an effort to curb infringement on its site." (Opp'n at 5.) The evidence establishes that Escape has recorded 37,986 account-holders for submitting works that were removed for possible infringement. If these 37,986 account holders were within Escape's cited 39,000 "terminated" accounts, and if termination resulted in deletion of the former account-holder's content, Grooveshark would lose approximately half of all the content in its active music library. (See SMF ¶¶ 138, 140.)

repeat infringers and allowing Escape to further profit from repeat infringers' content while at the same time facilitating Escape's attempt to seek safe harbor under § 512(c). While what constitutes termination under § 512(i) may differ from case to case, and may in some situation include disabling repeat infringers' uploading capabilities, the undisputed facts show that, under these circumstances, the DMCA requires more.

4. Conclusion as to "Implementation"

Courts have recognized a wide range of procedures and practices for implementing a repeat infringer policy that constitute "implementation" under § 512(i)(1)(A), and they should continue to do so. Thus, there is a high bar for a plaintiff to show that a service provider, as a matter of law, does not "implement" its repeat infringer policy within the meaning of the DMCA. The undisputed facts before the Court, however, point only to that conclusion. Escape does not have a repeat infringer policy or an alternative policy that serves the same purpose; does not keep records of repeat infringement sufficient to enforce an adequate repeat infringer policy; permits an extensive amount of repeat infringement to occur without taking action or making a record; depends upon a small number of repeat and flagrant infringers to supply a substantial amount of the content available on Grooveshark; takes action in response to copyright owners' DMCA notifications of infringement that fails to actually make the song unavailable or prevent it from reappearing immediately on Grooveshark; prevents copyright owners from collecting the data necessary to issue DMCA notifications in a meaningful way; and, finally, has never terminated a repeat infringer's account and has no policy or procedure for doing so. For these reasons in combination, the Court finds that Escape does not "implement" a repeat infringer policy under § 512(i)(1)(A) and is thus ineligible for DMCA safe harbor. Therefore, EMI's motion for summary judgment as to Escape's affirmative safe harbor defense should be granted.

ii. "Reasonable" Implementation

Escape's failure to implement a repeat infringer policy makes it ineligible for DMCA safe harbor and makes further inquiry into the § 512(i) prerequisites unnecessary. Nevertheless, in light of the scarce precedent for ending the inquiry before making a finding on the reasonableness of implementation, the Court discusses here whether, had Escape been found to implement its policy, that implementation was reasonable, i.e., carried out "in appropriate circumstances." Thus, for this discussion, the Court assumes that Escape's purported policy and practice of disabling the uploading capabilities of repeat infringers constitutes "termination" under § 512(i)(1)(A).

In response to EMI's evidence demonstrating the repeat infringers on Grooveshark whose uploading capabilities have not been disabled, Escape does not submit any evidence showing that it disabled the uploading capability of any Grooveshark account-holders, much less evidence showing that this policy was effected for repeat infringers.[22] As Escape would bear the burden at trial of establishing that it satisfies the DMCA's requirements for an affirmative safe harbor defense, Vimeo, 2013 WL 5272932, at *6, EMI's burden in its summary judgment motion "is satisfied if [it] can point to an absence of evidence to support an essential element of the non-movant's claim." Meltzer, 440 F. Supp. 2d at 187. EMI has satisfied this burden with respect to the element of "reasonable implementation."

In addition to the evidence showing Grooveshark users who infringed hundreds of works and who received multiple DMCA takedown notifications, the evidence also points to an

[22] Even if the Court were to consider the stricken Kowalski Declaration, this testimony would show only that "Escape has barred the uploading privileges of more than 38,900" account-holders. (Kowalski Decl. ¶ 6; see also id. ¶¶ 12-13.) In addition to providing no documentary evidence in support of this claim, Escape does not attempt to explain the circumstances under which it took this purported action. Thus, accepting Kowalski's testimony as true, there would still be no evidence that Escape ever disabled the uploading privileges for a repeat infringer, and no evidence on which the Court could assess whether the circumstances in which Escape carried out its policy were "appropriate" under the DMCA.

unknown number of infringers whose activity, and whether they are repeat infringers, cannot be determined as a result of Escape's DMCA Lite procedure. The DMCA Lite procedure, which does not result in recording the infringer or disabling her uploading ability, is not by itself unreasonable. Under the DMCA, a notification of claimed infringement is valid and may trigger an obligation on the part of the service provider only when it "includes substantially" six delineated components, including "[i]dentification of the material that is claimed to be infringing . . . , and information reasonably sufficient to permit the service provider to locate the material," and a statement affirming the notification signed under oath. 17 U.S.C. § 512(c)(3)(A); cf. CCBill, 488 F.3d at 1111-12 (finding that the knowledge requirements under § 512(c), which include knowledge stemming from valid DMCA notifications of infringement, also apply to a determination of whether a repeat infringer policy is implemented in "appropriate circumstances" under § 512(i)(1)(A)). According to Escape, it applies its DMCA Lite procedure when it receives non-compliant infringement notifications, e.g., when "they are not signed under oath or do not adequately identify the location of the alleged infringement on Grooveshark." (Opp'n at 39 (citing Tarantino Decl. ¶¶ 21, 22).)

The evidence demonstrates that, since February 13, 2013, Escape has removed 6,861 files, 94.2% of which it has removed under its DMCA Lite procedure. Escape has submitted no evidence demonstrating that any of the notifications of infringement with respect to these files were deficient, and the fact that the files were removed indicates that the notifications identified the allegedly infringing material and contained "information reasonably sufficient to permit" Escape "to locate the material." 17 U.S.C. § 512(c)(3)(A)(iii). Thus, the evidence demonstrates that, for 94.2% of the files removed for infringement, the submitting user's account was not terminated or recorded for determination of whether she is a repeat infringer, and there is no

documentary evidence demonstrating (1) that the DMCA notifications as to any of those files were deficient, or (2) that the removal of the remaining 5.8% of the files under the DMCA process resulted in Escape disabling the submitting users' uploading privileges. Accepting Escape's representation that the uploading privileges were revoked for the users who submitted those 5.8% of removed files, there is no evidence, and Escape does not contend, that any of those users were repeat infringers or among the small group of blatant infringers responsible for the vast majority of Grooveshark's infringing content. Thus, this evidence reveals a policy that is not implemented in "appropriate circumstances" or capable of determining when the circumstances would be appropriate, i.e., for cases of repeat and blatant infringement.

Further, Escape did not produce, either in discovery or in connection with this summary judgment motion, any records of DMCA notifications of infringements sent to users between November 16, 2010, and February 1, 2013; and Escape's database table used to log DMCA takedowns contains no entries from October 31, 2010 through March 20, 2012. As discussed, under Escape's DMCA takedown procedure, Escape purports to remove the allegedly infringing file, send a notification to the user who submitted the file, and disable the user's uploading privileges. Taken together, this evidence demonstrates a period of at least 16 months during which, at most, Escape removed user files under its DMCA Lite procedure, thus resulting in no notifications to the user, no record of the infringing user, and no disabling of any user's uploading privileges.[23]

Compounding the unreasonableness of Escape's policy, Escape does not take any action with respect to the thousands of non-primary files that are likely to be infringing where the

[23] This 16-month period is the overlapping time for which Escape produced no DMCA notifications of infringement and made no entries of DMCA takedowns in its database (November 16, 2010 through March 20, 2012). The period for which Escape produced no DMCA notifications sent to users – the more reliable indicator of whether Escape applied its DMCA or its DMCA Lite policy – is 26 months.

primary file is found to be infringing. Nor does Escape take any action with respect to users who submit an MP3 file with the same file hash as the file that was removed for infringement, despite the file hashes indicating that they are the exact same file and that the user is committing infringement. "[A] service provider may lose immunity if it fails to take action with regard to infringing material when it is 'aware of facts or circumstances from which infringing activity is apparent.'" CCBill, 488 F.3d at 1113-14 (quoting 17 U.S.C. § 512(c)(1)(A)(ii) and finding that Congress "imported [this] 'red flag' test . . . to the analysis of whether a service provider reasonably implemented its § 512(i) repeat infringer policy"); see also YouTube, 676 F.3d at 34-35 ("On this issue of first impression . . . , we hold that the willful blindness doctrine may be applied, in appropriate circumstances, to demonstrate knowledge or awareness of specific instances of infringement under the DMCA."); MP3tunes, 2013 WL 1987225, at *4 (withdrawing the court's previous grant of summary judgment in favor of defendant because of YouTube's holding that "something less than a formal takedown notice may now establish red flag knowledge"). Courts in the Second Circuit have interpreted the DMCA to allow for a narrow application of the doctrines of willful blindness and red flag knowledge, while recognizing the "tension" between these doctrines "and the DMCA's explicit repudiation of any affirmative duty on the part of service providers to monitor user content." Id. at *2 (citing 17 U.S.C. § 512(m)). In withdrawing its order granting summary judgment in favor of the defendant, the court in MP3Tunes noted that it does so "reluctantly" in light of the defendant's "salutary practice of sending instructions regarding DMCA-compliant takedown notices to third parties reporting possible infringement and the DMCA's disavowal of any duty on the part of service providers to monitor user content," as well as the rule that courts "'do not place the burden of determining

whether [materials] are actually illegal on a service provider.'" Id. at *4 (quoting CCBill, 488 F.3d at 1114).

Accordingly, the key fact here demonstrating unreasonableness under these doctrines is that while Escape's "matching" process, unless it fails to perform as intended, indicates that if a primary file is infringing, so too are the non-primary files, Escape takes no action regarding the non-primary files and *prevents* copyright owners from conducting any investigation into whether the non-primary files are infringing. Thus, Escape's willful blindness is not simply due to its failure to investigate whether the non-primary files are actually infringing, it is due to its active prevention of copyright owners from informing Escape that potentially thousands of files in the Grooveshark library are infringing. On these facts, Escape's repeat infringer policy cannot be found to be "reasonably implemented."

Finally, Escape's failure to show that it disabled the uploading privileges of any of the users who submitted EMI content after March 23, 2012, demonstrates unreasonable implementation. In the approximately 1.5 years following EMI's termination of its Distribution Agreement with Escape, Escape has uploaded to its servers 13,855 infringing files containing sound recordings owned by EMI, despite having the ability to filter those files and identify the infringing users. Escape, however, stopped filtering for EMI content after the termination of the Distribution Agreement and thus ignored circumstances in which users submitted content that was plainly infringing. Thus, Escape intentionally stopped conducting one of the few processes it had that could have allowed it to determine appropriate circumstances for implementing its repeat infringer policy.

Based on the foregoing facts, EMI has also carried its burden of establishing that Escape did not implement its repeat infringer policy in "appropriate circumstances" and thus did not

reasonably implement its policy. The undisputed evidence establishes that Escape does not satisfy either element of § 512(i)(1)(A)'s "repeat infringer policy" as a matter of law. Accordingly, Escape is ineligible for protection under any of the DMCA's safe harbor provisions. Therefore, EMI's motion for summary judgment as to Escape's DMCA safe harbor defense should be granted on the ground that Escape does not "implement" a repeat infringer policy, or, alternatively, that Escape's implementation of its repeat infringer policy is not reasonable. Because Escape cannot satisfy the prerequisites for a DMCA safe harbor defense, the Court makes no finding as to the requirements of § 512(c).

CONCLUSION

For these reasons, the Court recommends that EMI's motion for summary judgment be (1) DENIED as to its claim of direct infringement of its right of reproduction, and (2) GRANTED as to its remaining claims and as to Escape's affirmative defense of DMCA safe harbor.

NOTICE OF PROCEDURE FOR FILING OBJECTIONS TO THIS REPORT AND RECOMMENDATION

The parties shall have fourteen days from the service of this Report and Recommendation to file written objections pursuant to 28 U.S.C. § 636(b)(1) and Rule 72(b) of the Federal Rules of Civil Procedure. See also Fed. R. Civ. P. 6(a), (d) (adding three additional days when service is made under Fed. R. Civ. P. 5(b)(2)(C), (D), (E), or (F)). A party may respond to another party's objections within fourteen days after being served with a copy. Fed. R. Civ. P. 72(b)(2). Such objections shall be filed with the Clerk of the Court, with courtesy copies delivered to the chambers of the Honorable Alison J. Nathan at the United States Courthouse, 40 Foley Square, New York, New York 10007, and to any opposing parties. See 28 U.S.C. § 636(b)(1); Fed. R. Civ. P. 6(a), 6(d), 72(b). Any requests for an extension of time for filing objections must be

addressed to Judge Nathan. The failure to file these timely objections will result in a waiver of those objections for purposes of appeal. See 28 U.S.C. § 636(b)(1); Fed. R. Civ. P. 6(a), 6(d), 72(b); Thomas v. Arn, 474 U.S. 140 (1985).

SO ORDERED.

SARAH NETBURN
United States Magistrate Judge

DATED: New York, New York
May 28, 2014