UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

Case No. 11-20427-CIV-WILLIAMS

DISNEY ENTERPRISES, INC., *et al.*,

Plaintiffs,

vs.

HOTFILE CORP., *et al.*,

Defendants.
_____/

ORDER

THIS MATTER is before the Court on several pending motions for summary judgment, which were filed under seal and in a public, but redacted form (DE 255, DE 275, DE 276, DE 280, DE 301, DE 316, DE 318, DE 322). In connection with this briefing, the parties filed numerous related motions to strike (DE 217, DE 241, DE 339, DE 452, DE 371, DE 387), supplemental briefing permitted by the Court (DE 474, DE 475), and additional, robust pleadings on supplemental authority without leave of Court (DE 443, DE 444, DE 500, DE 501, DE 502, DE 503, DE 504, DE 505, DE 507, DE 509, DE 510, DE 513, DE 514, DE 515, DE 516, DE 517, DE 523).[1] Finally, the Court permitted the Electronic Frontier Foundation to file a brief as *amicus curiae* (DE 480). The Court addresses all related filings in this Order. To the extent that this Order discusses information considered by the parties to be business secrets, it will be redacted in a public version of this decision.

[1] As evinced by the volume of the briefing and the proceeding discussion, the parties do not agree on much, there are many facts asserted to be relevant, and the Court has been asked to weigh in on numerous unsettled legal issues.

I. BACKGROUND

This case concerns the actions of an off-shore technology company that provides online file storage services, Defendant Hotfile Corp., and one of its founders, Defendant Anton Titov (collectively, "Hotfile" or "Defendants"). Plaintiffs are five major media studios and entertainment companies (collectively, the "Studios") that hold copyrights on various artistic works: Disney Enterprises, Inc., Twentieth Century Fox Film Corporation, Universal City Studios Productions LLLP, Columbia Pictures Industries, Inc., and Warner Bros. Entertainment Inc. ("Warner"). The gravamen of the Studios' claim is that Hotfile's users have abused its system by sharing licensed materials belonging to the Studios and that Hotfile and Titov are liable as a result.

The pending motions for summary judgment seek an adjudication that Hotfile's activities are not (or are) entitled to a statutory safe harbor protection created by Congress fifteen years ago in the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 1201, *et seq.*; that Hotfile is (or is not) liable for secondary copyright infringement at common law; that Titov is (or is not) personally liable for Hotfile's activities as one of its corporate officers and founders; and that Warner is not liable for itself abusing a system that enabled it to remove works from Hotfile's system. After considering the extensive factual record and applying the relevant law, the Court concludes that Defendants have failed to meet criteria necessary for safe harbor protection; that Defendants are vicariously liable for the actions of Hotfile's users, but that questions of fact preclude a determination of other forms of secondary liability; that Titov is individually liable for the actions of his company, such that he will have to share in whatever judgment Hotfile is deemed to owe; and that Hotfile may proceed on a counterclaim it filed against Warner

relating to notices of infringement. This action will proceed to trial on all unresolved issues of liability as well as for a determination of the measure of damages.

A. Hotfile's System

Hotfile, which began its operations on February 19, 2009, is what is known as an online "storage locker." The company operates an Internet website that allows registered users to take electronic files of any type that are stored on their computers or other accessible locations and transfer them to Hotfile's electronic storage system through an uploading process. As a result, a copy of that file then exists on Hotfile's servers. The website provides a simple interface between Hotfile users (and their data) and Hotfile's storage network, connecting them with just a few computer mouse clicks. Once a file is uploaded, the uploading user automatically receives one or more unique URL links containing the file name and an extension. So, for example, if a user uploads a piece of software called "JDownloader" – which is a real program whose authors voluntarily uploaded it through Hotfile's website – Hotfile would issue the user a link location such as "http://hotfile.com/dl/14052520/7a3c8f8/JDownloader%200.8.821.zip.html." As can be seen, the link generally gives some indication of the file name, and thus, its possible content. By entering that link into the address bar of any Internet web browser on any computer, the user may retrieve and download his file. Hotfile keeps track of the date, time of use, and certain user information associated with the file.[2]

---

[2] This case revolves around emerging technologies, which requires the Court to give an overview of the relevant concepts. The parties have provided more comprehensive information and more sophisticated analyses, which are on file with the Court. (*See, e.g.,* Foster Decl. (DE 325-17).)

While an individual's act of uploading a file is ostensibly innocuous – and indeed, other networks provide similar sorts of services – several of Hotfile's attributes facilitate users' infringement of copyrights. First, while the uploading process places just one copy of the file on Hotfile's servers, that file can be downloaded an *unlimited* number of times. Moreover, there are no limitations as to how someone can further use or replicate the file.

Second, because the file is not secure, it is accessible to anyone with an Internet connection. It is important to note that Hotfile provides no index or search feature, which means that anyone trying to access a file must know its exact location or URL – the file is essentially hidden in plain sight. Nevertheless, ways exist for other users to learn about and gain access to files. For instance, Hotfile encourages users to share file links (and thus files) through an affiliate program, which pays individuals to navigate prospective downloaders to file locations. The incentives increase with the size of the file and the frequency of its download but without regard to other characteristics the file might possess (e.g., if it is entertainment media versus utility computer software or if it is created by the user or created by someone else).[3] In practice, Hotfile's affiliates have created their own websites that catalogue files found on Hotfile, promote their files, or allow the public to search for files. In addition, uploading users can themselves broadcast the download links, such as by e-mailing them to people they know or by

---

[3] The amounts paid per file – no more than $0.015 – are small, but in aggregate have resulted in the payment of millions of dollars to affiliates. Prior to 2012, Hotfile also paid website owners a five percent commission based on the number of users who purchased premium subscriptions to Hotfile and had been referred by such websites.

advertising them through various channels. This has turned Hotfile into not only a storage site, but also a file distribution network.

Finally, because Hotfile protects users' privacy, it has effectively refrained from interfering in any way with how its members use the service. In the normal course of its business, for example, Hotfile does not review what its users are uploading, downloading or promoting. Indeed, as discussed below, one of Hotfile's main defenses in this action is that it is unaware of the nature of the content available and has no affirmative duty to monitor user activities.

Hotfile has sought to increase the use of its system and expand the rate of file sharing because the corporation derives revenue through subscriber fees that users pay to it. Indeed, this is Hotfile's sole source of revenue. While Hotfile is accessible to the public and anyone can upload or download for free, paying nine dollars per month for "premium" status permits uploaders to store their files for a longer period; otherwise, files are automatically deleted every three months. Moreover, premium users who seek to download files benefit from easier access, faster download speeds, and the ability to download files frequently; they would otherwise be restricted to one download every thirty minutes. Hotfile calculates that user activity drives premium subscriptions while rewarding users for giving away access to files they possess. For instance, it is undisputed that Hotfile's affiliate program promotes the use of Hotfile and leads users to convert to premium status.

By any measure, Hotfile's model has been effective at encouraging user participation and driving growth among downloading users, uploading users and affiliate members. For instance, according to Hotfile's figures, 123 million files available on

Hotfile's system have been downloaded 2.9 billion times – 145 million times alone in the month preceding this lawsuit – and have resulted in the registration of 5.3 million users. (Titov Decl. ¶ 36 (DE 396-1).) This has worked a significant financial benefit to Hotfile and its founders. [redacted]

B. Legal Claims at Issue

As alluded to above, these features – the ease of replication and dissemination of any type of file, the lack of oversight regarding content, and the scale of Hotfile's activity – raise questions of liability for users' illegal activities.[4] In their Complaint filed on February 8, 2011 (DE 1), the Studios allege that while Hotfile proclaims to be an online personal storage site, it is actually designed to provide a mechanism for uploading and downloading users to engage in digital piracy, complete with a system of

---

[4] Systems with similar capabilities have faced careful scrutiny. For instance, in the late 1990s and early 2000s, copyright owners brought numerous successful challenges to peer-to-peer file networks, which coordinated the transmission of media stored on users' computers directly to other users, imposing liability on the network operators for the conduct of their users. *See, e.g., Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005); *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001); *Arista Records LLC v. Lime Group LLC*, 784 F. Supp. 2d 398 (S.D.N.Y. 2011) ("*Lime Group*"). The system challenged most recently, Megaupload Limited, shuttered its service in early 2012 and is facing potential criminal and civil liability in the United States. *See* Ben Sisario, *7 Charged as F.B.I. Closes a Top File-Sharing Site*, N.Y. Times, Jan. 19, 2012, at B1. While the parties have found it convenient to compare Hotfile to these systems, the Court predicates its decision on the facts and law presented by this record.

financial incentives that fosters infringement. They assert that it is Hotfile's infringing uses, not legitimate user activity, that drives the company's business. The Studios bring a claim for secondary infringement (Count II); their claim for direct infringement (Count I) was dismissed by prior order of the Court (DE 94). To frame the legal issues and put into context the evidence discussed throughout this decision, the Court provides the following summary of the parties' positions and their key evidence.

Although largely irrelevant to issues of liability, the cornerstone of the Studios' case is a statistical analysis conducted by Dr. Richard Waterman based on classifications provided by their proffered copyright expert, Mr. Scott A. Zebrak.[5] The report concludes that 90.2% of the daily downloads on Hotfile are downloads of "infringing" or "highly infringing" content and that only 5.3% of downloads are noninfringing, with a 1.3% margin of error. (Waterman Decl. ¶¶ 22-23 (DE 325-6).) The Studios also provide circumstantial and anecdotal evidence that Hotfile does not serve a

---

[5] As explained in more detail below, courts have squarely rejected the Studios' position that generalized evidence of infringement, such as Dr. Waterman's study, forecloses the statutory safe harbor protection afforded by the DMCA and necessitates a finding of liability. Although the Studios cite to dicta supporting the proposition that the goals of the DMCA are inconsistent with rewarding those who knowingly contribute to infringement (but mean to protect innocent actors who are engaged in beneficial applications of technology), a litigant must point to evidence of known infringement particular to works that they own. For instance, in *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19 (2d Cir. 2012), the Second Circuit found that a defendant could not be said to have awareness of infringement where an internal survey revealed that 75 to 80 percent of all content on the system was infringing. *Id.* at 32-34. As another case recently summarized, "knowledge of the prevalence of infringing activity, and welcoming it, does not itself forfeit the safe harbor. To forfeit that, the provider must influence or participate in the infringement." *Viacom Int'l, Inc. v. YouTube, Inc.*, No. 07 Civ. 2103 (LLS), 2013 WL 1689071, at *5 (S.D.N.Y. Apr. 18, 2013). Outside the scope of the DMCA, general knowledge of infringement is a factor supporting secondary liability for infringement but cannot establish such liability on its own.

primarily lawful purpose, as discussed below. Further, they contend that Hotfile knows about rampant infringement of works owned by the Studios and others, that Hotfile failed to remove infringing material or disable the accounts of users who uploaded such material despite having received eight million infringement notices from copyright holders, and that Hotfile and its uploading users have profited from the infringing activity. As a result, the Studios contend that Hotfile is liable under various theories of secondary copyright infringement and that it cannot avail itself of a safe harbor created in favor of service providers by Congress through Section 512 of the DMCA.

For its part, Hotfile portrays itself as anything but a pirate network. Hotfile and its founders claim that the corporation's business model is not unusual for the industry. And they contend that the system is used predominantly for storage and other legitimate uses, such as distributing non-licensed software; "space shifting" (i.e., enabling individual users to access their media through another device they own); and the sharing of media that is either created by users (such as videos to promote political change), freely licensed (or altogether not copyrighted), or too large to send by other methods. For example, Hotfile points to the fact tha[redacted]

Further, through its experts, Hotfile attempts to undermine the Studios' infringement analyses, contending that the Waterman study examined only a one-month period of data from January 2011 (leaving the possibility but hugely improbable

[6] No other Plaintiffs appear to have done so.

likelihood that there was a zero percent infringement rate in other months prior to this lawsuit) and improperly excluded entire categories of files, such as those with adult content, which is often given away with the copyright holders' permission, and public domain material, including works whose copyrights have expired. Hotfile does concede that, at least to some degree, infringement has occurred through its system and the availability of infringing files drives conversions to paid premium accounts. Nonetheless, to the extent that infringement did transpire on its system, Hotfile claims to have been unaware of it.

Hotfile also asserts that to the extent this litigation has highlighted ways it could better police the activity of its users, it has done so (even if it was not required to). This appears to be true. For example, when alerted by the Studios' lawsuit to the presence of infringing content, Hotfile implemented "powerful countermeasures" against Internet piracy, such as adopting filtering technologies and terminating large numbers of repeat infringers, that go beyond the most rudimentary foils to such activities. In this way, Hotfile advances the claim that it is a small, foreign company that has done everything possible to investigate its users' backgrounds, implement countermeasures to defeat piracy, and comply with United States copyright law (with which it says it was not always familiar). Finally, Hotfile asserts that the Studios have an improper motive in bringing this lawsuit, claiming that they stood witness to, and were complicit in, the alleged violations in order to drive damages and recover *post hoc*.

C. Evidence of Hotfile's Intent

The parties have diametrically different views of Hotfile's aims and have devoted much space to debating whether Hotfile set out to serve a legitimate purpose. Hotfile

acknowledges that at its inception, it modeled itself after RapidShare, another online storage locker website. Notably, copyright holders eventually claimed that RapidShare was used for infringement and brought suit against it in June 2010 to shut the network down. Hotfile was aware of RapidShare's problems. After the RapidShare lawsuit was filed, one of Hotfile's co-founders, [redacted], sent an e-mail to Titov noting an increase in traffic on Hotfile's system and remarking, "[w]hat an unexpected gift we have from Rapidshare :) The bad thing is that they clean up their image while we become the flagship of non-licensed content." (Yeh Decl. Ex. 53 (DE 288-58 (filed under seal; DE 324-11).) One month later, [redacted] speculated that one reason that "our profits increased so rapidly" was that "Hollywood has closed 3-4 large websites for illegal movies and that could have redirected users to us." (Yeh Decl. Ex. 49 (DE 288-54 (filed under seal); DE 324-11).) Titov responded to that e-mail by specifically naming RapidShare.

Apart from the generalized statistics highlighted earlier, the Studios have provided a pastiche of evidence related to Hotfile's business model, design and use that they contend makes a circumstantial case that Hotfile understood it was making illegal content available for distribution and tacitly fostering such activity. For instance, the fact that Hotfile encouraged downloading activity – by deleting files that are not frequently downloaded and by paying members only for downloading activity – means that Hotfile was intended to be a distribution network and not merely a storage facility. As a corollary, the Studios contend that Hotfile's affiliate compensation structure rewarded the sharing of *larger* and *popular* content, which drove premium conversions and earned revenue for the network.

On the other hand, Hotfile presents evidence that it conducts its affairs without regard to the nature of the content available on its system (i.e., protected by copyright or otherwise) or user activity (e.g., storage, sharing, streaming, etc.). Hotfile's expert, Dr. Boyle, challenges the Studio's claims about the conversion rate. Even the Studios' expert, Dr. Ian Foster, acknowledges that entertainment media, which may or may not be protected and which Hotfile users may or may not have had permission to share, can be a single large file, or "divided into several, smaller computer files in order to facilitate transmission or copying." (Foster Decl. ¶ 8 (DE 325-17).)

The Studios also point to specific documents to refute Hotfile's claims that it did not understand what was occurring on its system. For instance, in an e-mail between Hotfile engineers discussing the company's intellectual property policy, one of them stated that "what is protecting us legally is the fact that we don't know what is up there on our site. If we know, then we are susceptible to lawsuits. And now according to the IP policy, 10 days after a report, we pretend we don't know." (Yeh Decl. Ex. 54 (DE 288-59 (filed under seal); DE 324-11).) The Studios argue that Hotfile turned a blind eye to infringement. Moreover, as previously cited, Hotfile acknowledged (or at least expressed the concern) in the Summer of 2010 that it was becoming "the flagship of non-licensed content" and capturing infringing traffic from competing systems. And as discussed in the DMCA context below, Hotfile received millions of notices from copyright holders claiming that their rights to particular works were being infringed yet failed to target the associated users, failed to remove other identical copies of the works from the system (and only removed offending links and not the offending files), and did not implement robust counter-piracy tools until after this lawsuit was filed.

With regard to Hotfile's affiliate program, the Studios contend that because of "facially pirate" affiliate sites like "copymovie.net" – a website that, from screenshots, apparently displayed popular movies' promotional materials and may have been embedded with Hotfile download links – Hotfile should have understood the availability of copyrighted content. (Yeh Decl. Ex. 35 (DE 324-3).) In fact, Hotfile had several run-ins with affiliates regarding piracy. In one internal discussion, for example, an employee named "Andrei" reached out to Titov about an affiliate site called "PlanetSuzy" that was "converting well" but had somehow strained its relationship with Hotfile. Titov responded that "it must not appear in any way that we pay for advertising on a pornography site, where piracy activity prospers." (Yeh. Decl. Ex. 104 (DE 288-116 (filed under seal); DE 324-17).) While Hotfile suggests that the document shows its unwillingness to deal with infringers, the Studios provide evidence that "Hotfile most recently paid this affiliate during the period spanning January 16, 2012 through January 22, 2012 . . . suggesting that Hotfile is continuing to make payments to this website today." (Foster Decl. ¶ 56 (DE 286 (filed under seal); DE 325-17).)

The Studios also point to other Hotfile communications with affiliates. Instructions on Hotfile's system addressed to its affiliates stated that third-party site owners can get a commission equal to five percent of all premium accounts they sell, so those third-parties should "[p]ost *interesting* download links" in order to "earn big money." (Yeh Decl. Ex. 57 (DE 324-11) (emphasis added).) Other instructions to affiliates suggest uploading "files only if you inten[d] to promote them." (Yeh Decl. Ex. 59 (DE 324-11).) And, around the time of Hotfile's founding, someone affiliated with Hotfile, Andrew Ianakov, solicited affiliates by posting on a website that "[o]ur goal is to

reach people who are interested in this kind of business, and to find good uploaders . . . uploading some stuff – mp3, videos, applications, games on our file host and spread these links over . . . forums where download links are posted (to games, applications and so on)." (Yeh Decl. Ex. 60 (DE 324-12).)

Apart from affiliates, evidence of similar communications exists between Hotfile and its uploading and downloading users. One user seeking technical assistance, for instance, stated that "im a premium user n im trying to download from the below link but after clicking download button, page not found appears http://hotfile.com/dl/8651708/cad2aa3/Despicable.Me.2010.720p.BRRip.XViD.AC3-FLAWL3SS.part6rar.html." (Yeh Decl. Ex. 54 (DE 288-31 (filed under seal); DE 324-11).) Someone at Hotfile apparently responded with download instructions. The Studios contend that the file name identified above should have alerted Hotfile to the fact that a user was attempting to illegally download a portion of the popular movie *Despicable Me*. Beyond this example, the evidence shows that whenever Hotfile was contacted by users, the title of the file last accessed by that user was revealed.

In another document, a Hotfile user complained that he was unable to export files that had been uploaded from Hotfile to other services because those services "wrote me that all my files are BLACKLISTED." (Yeh. Decl. Ex. 1 (Titov Dep.) at 719:2-21. (DE 288-3 (filed under seal); DE 324-2).) Someone at Hotfile responded that "[s]ince the specific value is identical to a value marked *illegal* in our system, uploads are denied. We suggest to contact your hoster in this matter. Unfortunately, due to security and legal matters, the blockage of the value cannot be lifted." (*Id.* (emphasis added).) And Titov commented in an internal e-mail that "we generally do not support transferring files

from our system out and that is not a problem that we need to give much consideration." (*Id.* at 721:4-10.) In this regard, Hotfile argues that the files were non-transferrable for reasons independent of copyright; they were essentially blank files. But the Studios rejoin that the inference to be drawn is that Hotfile had notice that the user's files were infringing because they had been blocked by the other service.

Similarly, one portion of Hotfile's website allowed users to test whether a Hotfile link was operational. According to a screen shot, Hotfile provided the instructional example of "http://hotfile.com//dl/182987/c2d67b8/PCD.DollDomination.2009.rar.html." (Yeh Decl. Ex. 44 (DE 324-11).) The Studios contend that the link used as an illustration contained an album by "The Pussycat Dolls" called "Doll Domination" and that other copyrighted works were used in other tutorials illustrating Hotfile's functions. Hotfile argues that even if the file contained what the Studios assert it contained, this particular band authorizes certain works for online distribution, as one court has recognized. *See UMG Recordings, Inc. v. Veoh Networks, Inc.*, 620 F. Supp. 2d 1081 (C.D. Cal. 2008) (concluding that the defendant network did not have actual knowledge of infringing material where it knew that works by particular artists were available for download since they were uploaded by artists themselves, such as The Pussycat Dolls).

D. Additional Facts Relevant to Hotfile's DMCA Defense

As explained more fully below, Section 512 of the DMCA confers immunity "from all monetary relief" on Internet service providers that meet certain criteria with regard to storing infringing material and making it accessible. Principally, with respect to the network at issue here, a requirement for eligibility contained in Section 512(i) along with several other requisites contained in Section 512(c) mandate: that the defendant has a

policy, reasonably implemented, for terminating repeat infringers; that it is a qualified service provider; that it has properly registered a DMCA agent; that it does not have actual or "red flag" knowledge of the infringing nature of files stored on its system; that it takes down files that are the subject of an infringement notice; that it does not receive a direct financial benefit from the alleged infringing activity; that it does not have the practical ability to control the alleged infringements; and that it accommodates and does not interfere with standard technical measures used to protect content. Notably, the statute does not focus on the general characteristics of the network, does not require affirmative action to police content, and does not preclude a grant of immunity even if the operator knew or should have known of infringement generally. The parties' motions in this case concern in part whether Hotfile has met those requirements and, as a result, whether Hotfile became eligible for safe harbor protection at any point.

1. Infringement Notices and Hotfile's Repeat Infringer Policy

Under the DMCA, Internet service providers must reasonably implement a policy designed to terminate users identified as repeat infringers. To that end, since May 2010, Hotfile has provided its users with notice of a repeat infringement policy through the terms of service provided on its website. (Yeh. Decl. Ex. 1 (Titov Dep.) at 279:1-4 (DE 324-2).) That policy states that Hotfile "discontinue[s] service to users who repeatedly make such content available or otherwise violate HotFile's Terms of Service. Please do not abuse the HotFile service by using it to distribute materials to which you do not have the rights." (Titov Decl. ¶¶ 17-19 (DE 321-1).) Prior to that time, Hotfile had warned users that "[s]ervices of Hotfile can be used in legitimate objectives. Transmission, distribution, or storage of any materials that violate laws is forbidden.

This includes without restriction patented materials, copyright laws, trademarks, commercial secrets and other intellectual property rights." (*Id.* ¶ 12.) It had also posted an e-mail address on its website – abuse@hotfile.com – that the public could use to alert Hotfile of infringement. Although the policies essentially ask users not to engage in misconduct and warn that they may be excluded from using Hotfile, they are notably silent as to what criteria Hotfile would consider in terminating repeat infringers and what efforts it would undertake in doing so. It is undisputed that Hotfile terminated only approximately 43 users up to the filing of the Complaint.

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.[7] By the time this Complaint was filed, for instance, ten million such notices had been sent to the company with respect to links to files available on its system. (Foster Decl. ¶ 25 (DE 325-17) (discussing data produced by Hotfile).) Both sides agree that those notices correspond to approximately eight million unique files. (*Id.*; Titov Decl. ¶ 26 (DE 396-1).)

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). (Yeh. Decl. Ex. 1 (Titov Dep.) at 283:24-285:15 (DE 324-2).) Titov

---

[7] The DMCA sets out a notice protocol under which copyright holders can notify an agent responsible for the service of claimed infringement. *See* 17 U.S.C. § 512(c)(3); *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082, 1089 (C.D. Cal. 2001). The statute also allows service providers to challenge infringement designations through a counter-notification process.

said as much at his deposition, acknowledging that when Hotfile received a DMCA notice of infringement, it did not record which user it corresponded to:

> Q. Prior to the filing of this Complaint, when Hotfile received a DMCA notice from a copyright owner, did Hotfile attempt to identify the user who had uploaded the offending file?
>
> MR. THOMPSON: Objection, overbroad.
>
> A. I don't believe that would be the case most of the time. But again, on discretion, employees could investigate further.
>
> * * *
>
> Q. . . . . Absent a request, a specific request by a copyright owner, prior to the filing of this action, did Hotfile have a practice of identifying the user who had uploaded files identified as infringing on DMCA notices?
>
> MR. THOMPSON: Objection. Overbroad, asked and answered.
>
> A. I won't say "specific request," but if a copyright holder would raise some kind of concern that I – I think can be – can be summarized, again, a discretion, identification could be made.
>
> BY MR. FABRIZIO:
>
> Q. Okay. My question, though, is without a request from a copyright owner, when Hotfile received a DMCA notice, did Hotfile, as a matter of practice, identify the user who had uploaded the offending file?
>
> MR. THOMPSON: Objection. Asked and answered.
>
> A. I don't believe so.

(Yeh. Decl. Ex. 1 (Titov Dep.) at 281:10-282:15 (DE 324-2).) While Hotfile did not track such notices, Titov, as the designated corporate Rule 30(b)(6) representative regarding Hotfile's electronically stored information, testified that Hotfile knows the user identity for every upload and that it would have been a "trivial task" to extract user identities from infringement notices. (Yeh Decl. Ex. 2 (Titov ESI Dep.) at 51:23-52:4 (DE 288-4 (filed

under seal); DE 324-2).) In sum, prior to this action, whether a user was the subject of one notice or 300 notices, Hotfile acted no differently in terms of investigating possible infringement.

Instead, in its briefs, Hotfile credits a system of "manual review" and "discretion" for the termination of 43 users. However, the Studios' evidence demonstrates that Hotfile was motivated not by policy, but by the threat of litigation. Of those 43 terminations, 33 were due to a court's temporary restraining order issued in connection with litigation initiated by a pornography producer called "Liberty Media." (Yeh. Decl. Ex. 1 (Titov Dep.) at 299:1-24 (DE 288-2 (filed under seal); DE 324-2).) Others were apparently terminated when Hotfile or its affiliated entities received litigation threats from copyright holders. (*See, e.g., id.* at 306:12-307:10 (acknowledging that Hotfile terminated a user after a copyright owner complained of Hotfile's failure to respond to DMCA notices and threatening to hold Hotfile liable for "a huge loss to my company").) Thus, while Hotfile claims to have acted to "terminate, and stop payments to accounts of users with numerous complaints at content owners' request," it has failed to cite evidence to support the proposition, explain the conditions that led it to target or terminate users, or rebut the Studios' account of user termination only by litigation. (*See* Titov Decl. ¶ 34 (stating only that "Hotfile did review accounts of users with numerous complaints at the request of content owners, did perform manual reviews of those accounts, did terminate those accounts, and did stop payments") (DE 342-2 (filed under seal); DE 396-1).)

Similarly, Hotfile's public claims about its repeat infringer policy appear to be unfounded. For example, it purported to have a policy of automatically removing users

that had accumulated two "strikes," based on DMCA notices; the policy was discussed in internal e-mails. (*See* Liebnitz Ex. 29 (DE 346-31) at HF02835779 ("If user's files were reported two times as copyright abuse we delete user account.").) Hotfile also reported to copyright holders that it acted upon the notices of infringement that it received, but vetted them manually to ensure that the users it deleted had in fact infringed. (*Id.*) Likewise, internal documents suggest that Hotfile had a "system in place that flags the users [with] numerous infringing [Complaints]" and that the corporation "manually review[ed] those accounts," deleted them, and seized funds they have received from their affiliate program. (Yeh. Decl. Ex. 1 (Titov Dep.) at 286:6-18 (DE 288-2 (filed under seal); DE 324-2).)

In his deposition, Titov acknowledged that those representations were untrue. (*See, e.g.*, Yeh. Decl. Ex. 1 (Titov Dep.) at 286:6-289:4 (DE 324-2).) Indeed, had Hotfile paid attention to the DMCA notices, it would have known that by the time of the Complaint, 24,790 users had accumulated more than three notices; half of those had more than ten notices; half again had 25 notices; 1,217 had 100 notices; and 61 had more than 300 notices. (Foster Decl. ¶¶ 42-52 & Ex. D. (DE 286 (filed under seal); DE 325-17).) Moreover, documents produced in the litigation support the conclusion that, prior to the filing of the Complaint, Hotfile lacked any meaningful policy to combat infringement. Although it is the subject of a motion to strike on the grounds of hearsay and authenticity, one document purports to show a conversation thread in which a Hotfile user observes in an online forum that "[i]f any of you[r] files are reported by a real representative (see http://hotfile.com/reportabuse.html), then the file will be deleted, but your account will not be removed, and you will not be suspended from hotfile.com."

(Yeh. Decl. Ex. 22 (DE 288-25 (filed under seal); DE 324-2).) Similarly, another user who operated a site with Hotfile links, which the Studios suggest was "blatantly" infringing, was suspended but allegedly had his account restored after contacting Hotfile. (Yeh. Decl. Ex. 100 (DE 288-112 (filed under seal); DE 324-16).) The Studios' expert calculated that this particular user had uploaded nearly 30 thousand files to Hotfile and received [redacted] but had also accumulated 9,254 takedown notices. (Foster Decl. ¶ 54 (DE 286 (filed under seal); DE 325-17).) To the extent that they may be admissible at trial, these documents give substance to the Studios' assertions.

Like that user, the evidence produced shows that the subjects of the notices formed a discreet group of problematic users. While those who were the subject of more than three infringement notices made up less than one percent of all of Hotfile's users,[8] they were responsible for posting 50 million files (15.6 million of which were subsequently the subject of a takedown notice or removed for infringement), representing 44 percent of all files ever uploaded to Hotfile. (Foster Decl. ¶ 41 (DE 286 (filed under seal); DE 325-17).) Those same files were downloaded nearly 1.5 billion

[8] The fact that these users were few in number but had a large aggregate impact (particularly with respect to downloaded files) accounts for the discrepancies between the parties' proffered statistics, as does the fact that the Studios focus only on total downloading activity. For instance, Hotfile argues that only four percent of files ever uploaded have been the subject of a DMCA notice; that three percent have been removed by copyright holders under Hotfile's Special Rightsholder Account program; that the most popular downloads are not copyrighted; and that 56 percent of the files uploaded have never been downloaded. Further, because Hotfile made significant changes to its system after this lawsuit was filed, including implementing a three-strikes policy and various fingerprinting technologies to seek out infringing content, additional discrepancies are attributable to the time period analyzed. Supported by post-Complaint data, Hotfile asserts it has been more proactive in identifying and removing infringing files and users.

times, representing roughly half of all downloads ever from Hotfile. (*Id.*) [redacted] (*Id.*) In turn, the conversion rate evidence shows that Hotfile earned large sums from new premium users. Significantly, a snapshot taken by the Studios showed that their files accounted for one percent of the files on Hotfile, or 945,611 files. With regard to downloads, however, ten percent of files downloaded from Hotfile (according to the Studios' download study) were owned or controlled by the Studios.

While Hotfile's efforts to control infringers' activity appears to have been ineffective (whatever its policy might have been), Hotfile adopted a "revamped repeat infringer policy" immediately after this litigation began. The new policy focuses on "three strikes" – terminating and banning users who receive three DMCA notices of claimed infringement or Special Rightsholder Account requests (discussed below). (Titov Decl. ¶ 33 (DE 321-1).) Hotfile now tracks how many times it receives notices of infringement, each of which count as a "strike." (*Id.*) This revamped policy led directly to the termination of 444 of its 500 highest-paid affiliates, although thousands of smaller affiliates were not terminated. (Titov Decl. ¶ 30 (DE 396-1).) Ultimately, Hotfile terminated 22,447 users within months of the filing of the Complaint. (Titov Decl. ¶¶ 34, 37 (DE 342-1 (filed under seal); DE 396-1).) Hotfile cites this evidence in support of its argument that it is now DMCA compliant, while the Studios use the evidence to show how rampant and unchecked user activity had been. And Hotfile points out that the number of users removed is, in relative terms, a small number.

2. DMCA Agent Registration

Another requirement of DMCA protection is that a registered agent be designated to receive infringement notices. At least as far back as April 24, 2009, Hotfile maintained an e-mail address posted on its website for the public to report illegitimate or illegal user activity. At that time, the website explained to users that "[t]o exercise your DMCA rights, your Proper DMCA Notice must be sent to Designated Agent of hotfile.com to email: abuse@hotfile.com . . . When a Proper DMCA notification is received by Designated Agent, or when hotfile.com becomes aware that copyrights are infringed, it will remove or disable access to infringing materials as soon as possible." (Titov Decl. ¶ 15 (DE 321-1).) Hotfile formally registered a DMCA agent with the Copyright Office in December 2009, a fact that is undisputed. (Titov Decl. ¶ 16 (DE 321-1).) Thereafter, in May 2010, it posted a policy expressly incorporating the DMCA, informing users of its repeat infringer policy and the contact information for its designated agent. (Gupta Decl. Ex. 6 (Warner Interrog. Resps.) (DE 275-4 (filed under seal); DE 320-7).) It is further undisputed that the agent address provided by Hotfile was a post office box, which the Studios contend fails to comply with the statute.

3. Other Infringement Countermeasures

In addition to targeting repeat infringers' accounts, Hotfile makes much of other countermeasures it has put into place, largely after this litigation began. For instance, Titov stated that Hotfile's current practice is to remove individual files within 48 hours of receiving a notice, which he believes Hotfile does 95% of the time. (Titov Decl. ¶ 19 (DE 321-1).) The Studios do not dispute that since February 2011, Hotfile has adhered

to this practice, although the Studios have submitted documents suggesting that in some instances, Hotfile might not have always done so.

In August 2009, Hotfile implemented a Special Rightsholder Account ("SRA") program after receiving a request for a "takedown tool" from Plaintiff Warner. (Titov Decl. ¶ 20 (DE 321-1).). The program, which gives rise to Hotfile's counterclaim against Warner, allows trusted content owners who attest that they own rights to protected works to have access to Hotfile's system. This is a much quicker alternative than the user termination prompted by a DMCA-compliant infringement notice. Indeed, the parties have stipulated that notifications by the Studios through the SRA program have the effect of notices of infringement for purposes of the DMCA. (DE 151, at 2 ("Warner's notifications by means of Hotfile's SRA are (and have the effect of) notifications of claimed infringement to Hotfile's designated agent under 17 U.S.C. § 512(c)(3)(A), and are therefore subject to 17 U.S.C. § 512(f).").) Through an interface provided by Hotfile, owners are permitted to identify and automatically remove offending links without any action by Hotfile. According to record evidence, at least one of the Studios, Warner, has participated in this program.

Finally, Hotfile now actively polices files on its network, principally through advanced filtering technology. Video fingerprinting implemented in September 2011 is capable of identifying copyrighted content, which Hotfile claims to then block. (Titov Decl. ¶ 35 (DE 321-1).) Hotfile has also used so-called "hashing technology" (possibly since August 2009[9]) to remove identical copies of files once one is found to be infringing. This is a revision of the "master file policy" – something sharply criticized by

---

[9] While Titov stated in his declaration that the technology was implemented in August 2009, his deposition testimony is not consistent with that assertion.

the Studios – in which Hotfile saved server space by maintaining only one copy of identical files uploaded by different users. Formerly, when Hotfile received a claim of infringement, it disabled any offending links but did not actually remove the file from the server, thus leaving it accessible for download with a different link. And finally, Hotfile is employing other video and audio filtering technology that identifies files with characteristics matching content registered by copyright owners, which Hotfile then blocks. It is unclear what impact these technologies have had in blocking access to infringing files that were already available at the time the Complaint was filed. But, according to Hotfile, they have two significant, remedial outcomes: (1) Hotfile now removes all infringing files to the extent that its sophisticated technology can identify them; and (2) the low percentage of files currently identified and blocked (in the range of two to four percent in February 2012) demonstrates that Hotfile is no longer used to share infringing files. (*See* Gupta Decl. Ex. 38 (DE 321-39).)

E. Corporate History and Titov's Involvement

The Studios' last claim is against Titov individually because of his participation in, and ability to benefit from, the infringing activity present on Hotfile's network. In particular, paragraph 45 of the Complaint states that Titov adopted an infringement-reliant business model; designed the aforementioned affiliate program that promotes infringement and paid infringing users; planned technological features that both frustrated copyright enforcement and failed to prevent infringement by users; managed Hotfile's operations; and operated related businesses to evade liability. While Hotfile makes much of the fact that the Studios have been unable to prove up all of these

allegations, it is more significant that several of them are actually supported by the evidence produced in discovery.

As background, Hotfile is the successor to a business venture [redacted] Although it is unclear how Titov first became involved with [redacted] or what exactly the company was formed to do, it is undisputed that Titov performed software programing, search engine optimization and server administration for the company. At some point, [redacted] devised the idea for an online file hosting company based on a competitor in the market, Rapidshare. Thus, [redacted] provided the necessary start-up capital for Hotfile Corp. Titov was approached because of his technical expertise and prior web-hosting experience; he joined them in founding Hotfile in Fall 2008. Hotfile acknowledges that the [redacted] "researched the competition in this space to learn about the functionalities of other services" and agreed on Hotfile's business model. They then staffed the company almost entirely with [redacted] employees, who continue to work for Hotfile. (Yeh. Decl. Ex. 1 (Titov Dep.) at 105:5-7 (DE 288-1 (filed under seal); DE 324-2).)

The evidence shows that Titov's primary role at Hotfile is as a technical engineer, responsible for implementing business ideas and functions. For instance, the parties agree that Titov wrote the source code that runs Hotfile's website. (Yeh. Decl. Ex. 1 (Titov Dep.) at 497:3-7 (DE 288-2 (filed under seal); DE 324-2) (acknowledging writing between 50 and 70 percent of the source code); Yeh Decl. Ex. 88 (Titov Decl.) at ¶ 6 (DE 288-95 (filed under seal); DE 324-15) ("I wrote the source code for Hotfile's website with the assistance of one other person. We designed the source code from scratch.

My conservative estimate is that more than 1,000 hours have been spent developing the source code.").) Titov also provides "guidance" to [redacted] employees and oversees aspects of their work for Hotfile. (*Id.* at 132:8-20 ("I'm not sure that I do in fact supervise them but . . . to the extent they need some guidance and understanding of the technical parts of . . . our system, yes we do communicate, and – yes, I would say that I have certain authority over them.").)

The evidence demonstrates that Titov actively participates in the management of Hotfile and in decision-making. [redacted] Titov testified that Hotfile's [redacted] shareholders manage Hotfile jointly and, while the governance procedures have not always been formal, they agree on major decisions such as the implementation of Hotfile's affiliate program. (Yeh. Decl. Ex. 1 (Titov Dep.) at 597:11-598:22 (DE 324) (stating that "major issues" were put to a vote but were not opposed).) Additionally, Titov acknowledged that he received power of attorney to act on behalf of the corporation "as a manager of the company when [such] acts are authorized by other shareholders." (Yeh. Decl. Ex. 1 (Titov Dep.) at 79:23-80:1; 82:5-12 (DE 288-1 (filed under seal); DE 324-2).)

Nonetheless, it is undisputed that Titov does not have the authority to make unilateral decisions regarding important aspects of Hotfile's business or operations. Titov asserts that he was not the originator of certain concepts; for instance, he credits [redacted] with making the decision to implement the affiliate program. And Titov denies

involvement in other aspects crucial to Hotfile's business, such as soliciting new investors, selecting contractors or devising advertising strategies.

The evidence also shows that, in October 2009, Titov formed a company called Lemuria Communications Inc., a Florida corporation that Hotfile uses to perform web hosting, software maintenance and development. Titov, according to the Defendants, is "the sole owner, manager, and director" of Lemuria.[10] Lemuria, in turn, contracts with [redacted] to perform some of those services and pays for many of Hotfile's expenses. (Yeh. Decl. Ex. 1 (Titov Dep.) at 38:7-40:10, 106:2-107:14 (DE 288-1 (filed under seal); DE 324-2).)

Beyond examining Titov's overall responsibilities at Hotfile, the Studios point to several specific ways that Titov is linked to the infringement at issue. With respect to the affiliate program, which the Studios believe promotes infringement, it is undisputed that Titov provided input on technological feasibility. Moreover, Hotfile has failed to rebut the Studios' assertions that Titov paid affiliates from an account he opened and transferred to Hotfile Ltd., a company that handles most of Hotfile's finances and that he manages. (Titov Reply Decl. ¶ 4 (DE 378-1 (filed under seal); Yeh. Decl. Ex. 1 (Titov Dep.) at 602:9-14 (DE 324-2) ("Yes, there were instances where users were paid by an account opened [in] my name.").) Titov also stated that he was aware of the master file policy, acknowledging that it permitted users to continue to access suspected files even

[10] Lemuria was formed one month after Hotfile's previous Internet service provider informed the company that it had received a large number of infringement complaints from copyright holders and two months after a copyright holder served a subpoena on that Internet service provider. (Yeh. Decl. Ex. 1 (Titov Dep.) at 119:13-121(DE 288-2 (filed under seal); DE 324-2).) The Studios contend that Lemuria was formed to prevent the consequences of a third-party Internet service provider cutting off Hotfile's service and that Lemuria acts as a front for Hotfile's commercial activity. Hotfile denies these allegations.

while individual links were disabled. (Yeh. Decl. Ex. 1 (Titov Dep.) at 602:16-604:13 (DE 324-2).) Similarly, given that Hotfile was governed jointly, Titov did not recall opposing Hotfile's key policies, such as how it treated repeat infringers or how it endeavored to remove infringing files.

Finally, while evidence of Titov's personal involvement in Hotfile's treatment of copyright infringement claims is not extensive, he acknowledged instructing Hotfile employees to ban a user and to "[b]e more strict in stopping these days," after Hotfile was sued by a company called Perfect 10. (Yeh. Decl. Ex. 1 (Titov Dep.) at 317:15-321:10 (DE 288-2 (filed under seal); DE 324-2).) Titov was also responsible for hiring Hotfile's DMCA agent, but he claims that others are responsible for responding to DMCA notices and handling that aspect of Hotfile's operation.

F. Facts Relevant to Hotfile's Counterclaim

Separately, Warner moves for summary judgment on a 17-page counterclaim filed by Hotfile relating to 890 DMCA takedown notices that Warner submitted to Hotfile. (DE 161-4.) In these notices, Warner typically stated "under penalty of perjury" that it was "the owner or authorized legal representative of the owner of copyrights" and that it had "a good faith belief that use of this material is not authorized by the copyright owner, the copyright owner's agent, or the law." Since April 2009, Warner has participated in Hotfile's SRA program, in which the parties agree that deletions have the same legal effect as takedown notices.

The counterclaim asserts that the works at issue were mistakenly identified as infringing and that Warner violated 17 U.S.C. § 512(f) by making such knowing and material misrepresentations and causing injury to Hotfile. Warner contends that, while

mistakes were made, they were not made knowingly and are not the type of egregious violations contemplated by the statute; that there were few resulting damages to Hotfile; and that Hotfile's motive in pursuing the claim is to demonstrate how difficult it can be for anyone to identify and prevent infringement, which helps Hotfile illustrate its defense to the main infringement claims.

1. Warner's Review Process

Many of Hotfile's contentions concern the sufficiency of the review process Warner implemented to identify and notice particular files. As explained by Warner's head of anti-piracy operations, David Kaplan, Warner devotes the efforts of seven employees to online anti-piracy enforcement, hires third-party vendors, and, notably, uses the "common practice" of having "automated systems [ ] scan link sites and [ ] issue notifications of infringement to [storage] locker sites when infringing content is detected." (Kaplan Decl. ¶¶ 4-5 (DE 258 (filed under seal); DE 301-6).) This last practice is apparently the method by which the counterclaim files were selected for deletion and requires some explanation.

In the automated review process, Warner's employees first determine that a site is used for Internet piracy. (Kaplan Decl. ¶ 6 (DE 301-6).) They then manually create programmable instructions and matching criteria for "robots" – software programs that use keywords to search for content based on attributes such as the file's title, genre, and year of release. (Kaplan Decl. ¶¶ 7-9 (DE 258 (filed under seal); DE 301-6).) The robots then, on their own, use search algorithms to spot URL links to infringing content. The search instructions are refined based on how often they improperly detect non-Warner content that appears in the robots' search results. (*Id.* ¶ 8.)

[redacted] For each link determined to contain infringing content, Warner sends infringement notices.

2. Prevalence and Knowledge of Errors

Overall, while the evidence shows that Warner's system has many commendable characteristics, it also reveals some areas for improvement. On one hand, Warner applies the system only to sites it believes to be devoted to infringing content, takes care in [redacted] uses employees to tailor search terms, [redacted], reviews its practices on a continuous basis, conducts spot checks, [redacted] (Kaplan Decl. ¶¶ 15-16 (DE 301-6).) Warner contends that it "has designed its system to err on the side of conservatism, even if that results in fewer infringing files being identified, in order to avoid errors," and professes great confidence in the reliability of its enforcement. (*Id.* ¶ 6.) It also repeatedly asserts that its methodology and system features are common in its industry.

On the other hand, Warner readily admits that mistakes do occur, and Hotfile has identified characteristics that may be responsible for engendering those mistakes. For example, Warner's staff did not download or review any Hotfile content before marking it

for removal. (Thompson Decl. Ex. 4 (Kaplan Dep.) at 43:12-44:14 (DE 354-5).)[11] Indeed, its search process relied on computer automation to execute programs and did not involve human review of the file titles, page names or other overt characteristics before issuing a takedown notice. And because the files were not reviewed, neither Warner's robots nor its employees made a determination whether there were legal uses for the files.

The parties have proffered limited statistical and anecdotal evidence about how this translates to the effectiveness of Warner's system. For its part, Warner avers that it sent 400,000 takedown notices to Hotfile prior to this lawsuit without receiving any counternotices from Hotfile or its users, suggesting that the mistakes were not apparent or significant enough to contest. (*See* Kaplan Decl. ¶ 14 (DE 301-6).) Moreover, according to Warner, the fact that only 890 erroneous files have been identified by Hotfile after it undertook the most scrupulous review of those takedown notices suggests a low error rate, well under one percent, by a simple calculation.

Warner goes further, suggesting that the actual number of mistaken notices sent to Hotfile numbers around 600, not 890. Showing the difficulty attendant to identifying infringing content, the evidence shows that 19 of the files challenged by Hotfile in the counterclaim are in fact owned by Warner. Another 271 of the files undisputedly belong to an entity, Electronic Arts, Inc., that gave Warner permission – albeit, apparently after-the-fact – to request removal of the files. (*See* Hopkins Decl. ¶ 9 (DE 301-7) (Electronic

---

[11] Warner contends that it would not have been "practicable for Warner to download files prior to issuing a notification of infringement" because of the computing resources required. (Kaplan Decl. ¶ 17 (DE 301-6).) Additionally, some of the files in the counterclaim were reviewed by a Warner vendor called LeakID, which does use a human screening process. (*Id.* ¶ 20.)

Arts, Inc. executive stating that the company "retroactively authorizes Warner having sent takedown notices" on its behalf).) And it is also undisputed that of the 890 files listed, 24 are duplicative. This further supports the view that Warner's actual error rate, in general and with respect to its search of Hotfile's website in particular, is small.

In response, Hotfile points to other evidence that Warner's error rate may actually be higher, the most important being an internal discussion between Warner employees in August 2011. [redacted] Thus, drawing inferences in favor of Hotfile, Warner employees might have known of an error rate as high as [redacted] during the time that it was identifying the files identified in the counterclaim.

Hotfile also points to instances of anecdotal errors to show how unsound Warner's search practices might have been. For example, [redacted] (Thompson Decl. Ex. 4 (Kaplan Dep.) at 16:10-17:4 (DE 354-5).) Warner also apparently [redacted] (Thompson Decl. Ex. 5 (DE 304-1 (filed under

seal); DE 354-6).) A search for the [redacted] (Thompson Decl. Ex. 16 (DE 304-6 (filed under seal); DE 354-17).) And [redacted] (Thompson Decl. Ex. 18 (DE 304-6 (filed under seal); DE 354-19).)

Moreover, Warner admits that on linking sites, it [redacted] (Thompson Decl. Ex. 4 (Kaplan Dep.) at 232:23-233:7 (DE 304-1 (filed under seal); DE 354-5).) Thus, it deleted one of the counterclaim files because it [redacted] Hotfile claims that *en masse* deletion was Warner's typical practice and extends beyond this example.

In addition, Hotfile has also proffered evidence of an illicit motive on Warner's part. For example, Warner liberally removed what is by all indications a popular and innocuous free software program mentioned at the outset of this decision, JDownloader, which was created by a company called "Appwork GmbH" and which Warner does not own or have rights to. In one instance, Warner targeted the program because it [redacted] (Thompson Decl. Ex. 4 (Kaplan Dep.) at 225:13-226:12 (DE 304-1 (filed under seal); DE 354-5).) [redacted]

proximity would "help people download the pirated version more rapidly." (*Id.* at 225:13-21.) Kaplan acknowledged that this resulted in Warner deleting something it did not have rights to, but later denied the removal was intended. (*Id.* at 226:4-12, 236:9-18.)

Warner's efforts to police were at times overzealous and overreaching. In the case of JDownloader, its anti-piracy executive stated that despite not owning the program he could not "say that [Warner] would have no legal right to take down JDownloader in some circumstances at least" under Section 512(c). (Thompson Decl. Ex. 4 (Kaplan Dep.) at 236:9-18 (DE 304-1 (filed under seal); DE 354-5).) As discussed above, Warner took liberties in removing content owned by other copyright holders, such as Electronic Arts, only obtaining permission to do so later in an "antipiracy partnership." In the main summary judgment briefing, the Studios show that the most popular content on Hotfile is actually software that is illegal to distribute but that does not include the Studios' works. And, in its motion, Warner points out that Hotfile is unable to recover for the vast majority of the files Warner wrongfully removed. These facts demonstrate that Warner's goals may have been broader than preventing infringement of its own works in the manner prescribed by Section 512(c).

3. Evidence of Damages

Assuming Warner's actions were unauthorized, Warner contends that Hotfile is unable to show a cognizable injury from the takedown notices identified in the counterclaim. First, Warner has established that many of the files did not cause Hotfile to wrongfully terminate any paying users. At least 28 of the files were noticed before Hotfile implemented a repeat infringer policy based on strikes, meaning that Hotfile took no action when it received those notices. Similarly, nine files wrongfully noticed after

Hotfile implemented its three-strikes policy in February 2011 did not result in user termination, since those users never accumulated more than three strikes. Additionally, 53 files were posted by users who would have accumulated three or more strikes without counting the files from the counterclaim, although Hotfile questions whether some of those notifications were DMCA-compliant. And finally, nine remaining files correspond to six users, none of whom was a subscribing member. These facts are not otherwise subject to dispute.

Warner has also retained an expert, Dr. Zebrak, who concluded that 477 of the files – if they did not belong to Warner – "highly likely" infringed others' copyrights and had no business being on Hotfile's system. This portion of Dr. Zebrak's testimony is challenged by Hotfile, which points out that the expert acknowledged he did not contact those owners to find out whether distribution on Hotfile was truly unauthorized. (Zebrak Decl. ¶ 16 (DE 201-1); Thompson Decl. Ex. 32 (Zebrak Dep.) at 319:3-22 (DE 354-33).) It is well-established that a lack of authorization is required to prove a claim of copyright infringement. *See Morley Music Co. v. Cafe Cont'l, Inc.*, 777 F. Supp. 1579, 1582 (S.D. Fla. 1991) (citations omitted). There is no compelling evidence one way or the other establishing these files' copyright status.

But Hotfile's main assertion is that Warner's focus wrongly assumes that Hotfile's lost revenue could only have come from terminated users' subscription fees. Instead, Hotfile points out that its business model is driven by the availability of content, which Warner's actions have interfered with. Hotfile has provided evidence that the files in the counterclaim, even excluding the files identified as infringing by Dr. Zebrak, were downloaded 278,319 times and earned Hotfile [redacted] in premium subscriptions from 51

new user accounts. (Titov Decl. ¶¶ 7-8 (DE 304-10 (filed under seal); DE 352-1).) The JDownloader program in particular was deleted eight times by Warner, but had been downloaded a total of 150,028 times and resulted in 42 premium subscriptions, earning [redacted] for Hotfile. (Titov Decl. ¶¶ 7-8 (DE 304-10 (filed under seal); DE 352-1).) And, Warner's own expert acknowledged that the false notices caused one JDownloader distributor to be briefly suspended, apparently preventing downloads of his files for two days. It is unclear whether the files deleted were ever replaced. (Foster Reply Decl. ¶ 3 (DE 360-1 (filed under seal); DE 409-9).)

Hotfile's expert, Dr, Matthew R. Lynde, estimates that Hotfile's total damages range from [redacted]. (Thompson Decl. Ex. 34 (Lynde Decl.) at ¶ 9 (DE 304-7 (filed under seal); DE 354-35); Yeh. Decl. Ex. 1 (Lynde Dep.) at 282:5-25 (DE 301-10).) He opines on a variety of ways in which Hotfile could have been harmed, including diminishing payments to affiliates, decreasing incentive for users to pay for premium access, and harm to Hotfile's business reputation and goodwill. His opinion associates an observed decrease in revenue with increased use of takedowns by Warner.

II. DISCUSSION

The parties have moved for summary judgment on various aspects of the claims and defenses raised in this litigation. Under Federal Rule of Civil Procedure 56, summary judgment is appropriate if, after discovery, "the pleadings, depositions, answers to interrogatories, affidavits and admissions on file, together with the affidavits, show that there is no genuine issue as to any material fact and that the moving party is entitled to a judgment as a matter of law." *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986) (quoting Fed. R. Civ. P. 56(c)). "An issue of fact is 'material' if, under the

applicable substantive law, it might affect the outcome of the case." *Hickson Corp. v. N. Crossarm Co., Inc.*, 357 F.3d 1256, 1259-60 (11th Cir. 2004) (citations omitted). "An issue of fact is 'genuine' if the record taken as a whole could lead a rational trier of fact to find for the nonmoving party." *Id.* at 1260 (citations omitted). "The moving party bears the initial burden of establishing the nonexistence of a triable fact issue." *Cont'l Cas. Co. v. Wendt*, 205 F.3d 1258, 1261 (11th Cir. 2000) (citing *Celotex Corp.*, 477 U.S. at 317). In ruling on summary judgment, the evidence and reasonable inferences are construed in the light most favorable to the non-movant. *Adickes v. S.H. Kress & Co.*, 398 U.S. 144, 157 (1970); *Jackson v. BellSouth Telecomms.*, 372 F.3d 1250, 1280 (11th Cir. 2004).

If the movant establishes the absence of a genuine issue of material fact, the nonmoving party must "go beyond the pleadings and by her own affidavits or by the 'depositions, answers to interrogatories, and admissions on file' designate 'specific facts showing that there is a genuine issue for trial." *Celotex*, 477 U.S. at 324 (quoting Fed. R. Civ. P. 56(c)). Thus, "[i]f the non-movant . . . fails to adduce evidence which would be sufficient . . . to support a jury finding for the non-movant, summary judgment may be granted." *Brooks v. Blue Cross & Blue Shield of Fla., Inc.*, 116 F.3d 1364, 1370 (11th Cir. 1997) (citation omitted). However, "if factual issues are present, the Court must deny the motion and proceed to trial." *Warrior Tombigbee Transp. Co. v. M/V Nan Fung*, 695 F.2d 1294, 1296 (11th Cir. 1983) (citations omitted).

A. DMCA Defense

The parties agree that the proper starting point for the Court's analysis is whether Hotfile is entitled to DMCA protection, given its ability to absolve Hotfile of liability for

secondary copyright infringement. *See* 17 U.S.C. § 512(c)(1) (stating that if the safe harbor requirements are met, "[a] service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright 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."); S. Rep. No. 105-190 (1998) at 64, reprinted in 1998 U.S.C.C.A.N. at 639 (stating that the safe harbor "protect[s] qualifying service providers from liability for all monetary relief for direct, vicarious and contributory infringement" as well as injunctive relief). As recounted in detail in *Viacom*, Congress enacted the DMCA in 1998 to provide liability safe harbors for service providers that operate or control networks through which users store copyrighted digital works if those providers meet certain specified criteria. 676 F.3d at 26-27 (citing 17 U.S.C. § 512(a)-(d) and legislative history). The Studios contend that Hotfile is not entitled to safe harbor protection as a matter of law, while Hotfile asks for a determination that it is not liable for acts of infringement that took place after the filing of the Complaint on February 18, 2011.

Generally, the advances of the Internet and digital technology make possible replication and dissemination of creative works on an astonishing scale. S. Rep. No. 105-190 (1998) at 8 (noting "the ease with which digital works can be copied and distributed worldwide virtually instantaneously"). In that regard, the DMCA was meant to foster the growth of the Internet while protecting the rights of copyright holders and encouraging Internet entities' efforts to offer valuable on-line services, which on occasion might be infringing under copyright law. *Id.*; *Realnetworks, Inc. v. DVD Copy Control Ass'n*, 641 F. Supp. 2d 913, 943 (N.D. Cal. 2003) ("The DMCA represents

Congress' attempt at a balance to preserve ownership rights protection for companies and artists in the face of the modern reality of a digital world with an increasingly technologically-savvy population."). As Hotfile recognized at oral argument, without the immunity conferred by the DMCA safe harbor provisions, Internet businesses could otherwise be subject to ruinous liability under common law principles of secondary infringement.

A party asserting DMCA's safe harbor as an affirmative defense to a claim of copyright infringement has the burden of demonstrating entitlement to its protections. *See ALS Scan, Inc. v. RemarQ Communities., Inc.*, 239 F.3d 619, 625 (4th Cir. 2001) (stating that entitlement to immunity under the DMCA is not "presumptive" but applies to service providers that prove they meet certain criteria); *see also Blue Cross & Blue Shield of Ala. v. Weitz*, 913 F.2d 1544, 1552 (11th Cir. 1990) (discussing burden of proof as to a statute of limitations defense). Nonetheless, in many instances, the DMCA serves to relieve service providers of burdens they might otherwise shoulder, even transferring them to the copyright owner. *See, e.g., UMG Records, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013) ("Congress made a considered policy determination that the 'DMCA notification procedures [would] place the burden of policing copyright infringement — identifying the potentially infringing material and adequately documenting infringement — squarely on the owners of the copyright.'" (quoting *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1113 (9th Cir. 2007))). In this regard, courts have counseled that the advantages of the DMCA should be viewed capaciously. *See Flava Works v. Gunter*, 689 F.3d 754, 758 (7th Cir. 2012). Although

an affirmative defense, the DMCA has often been construed in favor of service providers, requiring relatively little effort by their operations to maintain immunity.

Hotfile asserts that it qualifies for DMCA protection as an Internet service provider that allows information to reside on its system at the direction of its users, which is one of four specified categories recognized by the Act. *See* 17 U.S.C. § 512(c)(1). The parties do not dispute that Hotfile qualifies as a service provider. *See id.* § 512(k)(1)(A) (defining a "service provider" as "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received."). The term "storage" has also been broadly interpreted to include displaying or disseminating content that is uploaded to the system's servers at the direction of users, which covers Hotfile's operations. *See UMG Recordings, Inc.*, 620 F. Supp. 2d at 1089-91 (construing statutory language and concluding that Congress intended a broad application by including the phrase "by reason of," such that the protected infringing conduct need not be limited to an act of storage).

Section 512 provides that a preliminary condition for eligibility is that the service provider maintain a policy to terminate "repeat infringers." 17 U.S.C. § 512(i)(1)(A). The particular category of service provider that applies to Hotfile imposes four additional requirements: (1) the service provider designates an agent to the United States Copyright Office and to the public through its service; (2) the service provider acts expeditiously to "remove, or disable access to" infringing material it actually knows of or of which it should be aware from "facts or circumstances" showing that "infringing

activity is apparent;" (3) the provider has no actual or red flag knowledge of infringing activity; and (4) the provider receives no financial benefit from infringing activity. *Id.* § 512(c)(1). While case law has developed in other parts of the country, construing these provisions is an issue of first impression in this Circuit.

1. Repeat Infringer Policy

The repeat infringer requirement of Section 512(i) calls for a policy, reasonably implemented, that provides for the termination of a service provider's users in "appropriate circumstances":

> The limitations on liability established by this section shall apply to a service provider only if the service provider . . . 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). Congress, in enacting the DMCA, failed to elaborate upon what it means for a policy to be reasonably implemented. *See Perfect 10, Inc. v. CCBill, LLC*, 488 F.3d 1102, 1109 (9th Cir. 2007). Thus, in the absence of express statutory language, the Ninth Circuit has prescribed that "an implementation is reasonable if, under 'appropriate circumstances,' the service provider terminates users who repeatedly or blatantly infringe copyright" – a standard that this Court applies. *CCBill, LLC*, 488 F.3d at 1109 (quoting legislative history).

Such a policy may take a variety of forms. *Id.* Notably, "§ 512(i) does not require a service provider to decide, *ex ante*, the specific types of conduct that will merit restricting access to its services." *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1101-02 (W.D. Wash. 2004), *rev'd in part on other grounds, Cosmetic Ideas, Inc.*

v. IAC/Interativecorp., 606 F.3d 612 (9th Cir. 2010). For storage lockers like Hotfile, the focus of the analysis is on uploading users: "users who know they lack authorization and nevertheless upload content to the Internet for the world to experience or copy . . . are blatant infringers that Internet service providers are obligated to ban from their websites." *Capitol Records, Inc. v. MP3tunes, LLC*, 821 F. Supp. 2d 627, 637 (S.D.N.Y. 2011).

In assessing the reasonableness of a defendant's efforts, additional guidance on what constitutes an appropriate policy can be ascertained in the Act's legislative history. For instance, policies should be considered in light of Congress's intention 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." *UMG Recordings, Inc. v. Veoh Networks, Inc.*, 665 F. Supp. 2d 1099, 1118 (C.D. Cal. 2009) (quoting legislative history). Service providers granting access to those users should also be given "strong incentives . . . to prevent their services from becoming safe havens or conduits for known repeat copyright infringers." *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1178 (C.D. Cal. 2002). Yet consonant with other provisions of the DMCA, courts should not construe policies so as to impose affirmative action on the part of the service provider to monitor for infringement. *See* 17 U.S.C. § 512(m); *Cybernet Ventures, Inc.*, 213 F. Supp. 2d at 1176 (interpreting legislative history). As Congress stated:

> The Committee recognizes that there are different degrees of on-line copyright infringement, from the inadvertent and noncommercial, to the willful and commercial. In addition, the Committee does not intend this provision to undermine the principles of new subsection ([m]) or the knowledge standard of new subsection (c) by *suggesting that a provider must investigate possible infringements, monitor its service, or make*

> *difficult judgments as to whether conduct is or is not infringing*. However, 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.

H.R. Rep. No. 105-551(II) at 61 (1998) (emphasis added).

The Studios in this action do not contend that Hotfile failed to dictate or publish any policy, but rather that Hotfile failed to reasonably implement it by actually terminating users. Several considerations, taken together, lead the Court to agree. Initially, a reasonable policy must be capable of tracking infringers. Reviewing the holdings of *Ellison v. Robertson*, 357 F.3d 1072 (9th Cir. 2004) and *In re Aimster Copyright Litigation*, 334 F.3d 643 (7th Cir. 2003), *cert. denied*, 540 U.S. 1107 (2004), the court in *CCBill* announced a standard for Section 512(i) in which a service provider must maintain a vehicle to receive notices of potential infringement, design its system so as to be able to ascertain the identity of the users responsible for those files, and make some effort to record infringing users. 488 F.3d at 1110.[12] Without those threshold functions, service providers are unable to carry out any sort of reasonable policy. For instance, in *In re Aimster Copyright Litigation*, 252 F. Supp. 2d 634 (N.D. Ill. 2002), the district court concluded that whatever policy the defendants might have ostensibly had could not be reasonably implemented because the system's encryption

---

[12] This is different from a situation where a plaintiff claims that a service provider must look for repeat infringers who open accounts under new pseudonyms. *Cf. Io Grp., Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1144-45 (distinguishing *A&M Records, Inc. v. Napster, Inc.*, No. C99-05183 MHP, 2000 WL 573136 (N.D. Cal. May 12, 2000), which found that failure to block users' Internet Protocol addresses created a question whether the policy was reasonable). In *CCBill*, there was no dispute that the defendant implemented a policy by which it kept a DMCA log indicating the name and e-mail address of the webmaster for each site to which it provided service.

of user information made it "impossible to ascertain which users are transferring which files." *Id.* at 659. The court ruled that the precondition to safe harbor was not met even though the plaintiffs had failed to identify "a single repeat infringer whose access should be terminated." *Id.*

In this case, while the statute does not require Hotfile to maintain a perfect policy (or even anything as stringent as the three-strikes policy it eventually implemented), it is apparent that Hotfile effectively did nothing to tie notices to repeat infringers. Titov admitted, and Hotfile does not seriously dispute, that the corporation had no way to keep track of infringing users based on infringement notices. Hotfile's sole method for terminating its users was its "discretion," which it evidently failed to exercise; it had no technology to record notices and no procedure for dealing with notification. Consequently, it is not too harsh an assessment to conclude that when Hotfile received such notices, it was Hotfile's practice to ignore them rather than act to terminate the users they were associated with. This deliberate disregard is significant.

The data discussed above – both the number of users who received multiple notices of infringement and the number of users who were terminated after Hotfile implemented a stronger policy – show that Hotfile failed to act when confronted with infringing conduct.[13] Thus, despite receiving over eight million notices for five million users, Hotfile only terminated 43 users before the commencement of this action, for reasons that had no apparent relation to the notices Hotfile received. Most glaringly, there were 61 users who had accumulated more than 300 notices each. As recounted

---

[13] Hotfile claims that it "had no knowledge that the file[s]-in-suit were infringing *apart* from notifications Hotfile [might] have received from the Studios regarding these alleged infringements." (Titov Decl. ¶ 6. (DE 321-1) (emphasis added).)

above, those users were particularly prolific, driving traffic to Hotfile's website, receiving money through Hotfile's affiliate program, and generating significant revenue for Hotfile by encouraging users to convert to premium subscriptions.

In response, Hotfile contends that the DMCA does not mandate action based on infringement notices. On this point, there is some disagreement as to whether such notices equate to knowledge of a user's actual infringement.[14] *See, generally,* 4-12B M; Nimmer & Nimmer, Copyright § 12B.10[B] (Matthew Bender Rev. Ed. 2013). The court in *Corbis Corp.*, for instance, found that DMCA notices alone are not enough to confer knowledge on a service provider: "Although there may be instances in which two or more DMCA compliant notices make a service provider aware of a user's blatant, repeat infringement, the notices alone do not make the user's activity blatant, or even conclusively determine that the user is an infringer." 351 F. Supp. 2d at 1105 & n.9; *see also MP3tunes, LLC*, 821 F. Supp. 2d at 637.

Yet a subsequent circuit court decision in *CCBill* suggests a different approach on this issue. That court held that statutorily *deficient* notices of infringement – in particular, those lacking a declaration from the copyright holder detailing ownership and the material's infringing nature – were an insufficient basis for terminating a user. *CCBill*, 488 F.3d at 1113. At the same time, however, it held that the district court erred in failing to consider whether defendants' continued services for websites that were the subject of non-party notifications (which might have conformed with the statute)

---

[14] Courts agree that Section 512(i) requires terminating *known* repeat infringers. *See CC Bill*, 488 F.3d at 1113 ("A policy is unreasonable only if the service provider failed to respond when it had knowledge of the infringement."); *Ellison*, 357 F.3d at 1080.

constituted an unreasonable policy. *Id.* Thus, the decision suggests that *proper* notifications, which require "[a] statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law," 17 U.S.C. § 512(c)(3)(A)(v), can provide requisite knowledge to defendants. Other decisions support this reasoning. *See UMG Recordings, Inc.*, 665 F. Supp. 2d at 1116-18 (holding that filtering technology used by the defendant to identify infringing material did not constitute knowledge because, "however beneficial the [filtering] technology is in helping to identify infringing material, it does not meet the standard of reliability and verifiability required by [*CC Bill*] in order to justify terminating a user's account"); *Flava Works, Inc. v. Gunter*, No. 10C6517, 2011 WL 3205399, at *10 (N.D. Ill. July 27, 2011), *rev'd on other grounds*, 689 F.3d 754 (7th Cir. 2012) ("It is true that service providers are not required to police their sites for infringement, but they are required to investigate and respond to notices of infringement — with respect to content *and* repeat infringers."). As one court observed, *CC Bill* borrowed the knowledge standard from Section 512(c)(1)(A), which requires removal of material upon notification of *claimed* infringement. *UMG Recordings*, 665 F. Supp. 2d at 1117; *see also Corbis Corp.*, 351 F. Supp. 2d at 1107 ("[T]he most powerful evidence of a service provider's knowledge [is an] actual notice of infringement from the copyright holder."); *cf. UMG Recordings, Inc.*, 2013 WL 1092793, at *10 (stating that the plaintiff's "decision to forgo the DMCA notice protocol stripped it of the most powerful evidence of a service provider's knowledge – actual notice of infringement" (quotation omitted)).

Aside from infringement notices, however, Hotfile had no alternative method for preventing repeat infringement by its users. Courts often consider the degree of

infringement at issue and the defendant's efforts to stop repeat infringers in determining the reasonableness of the policy's implementation. In *Corbis Corp.*, for instance, the defendant had cancelled millions of offending merchant listings, warned such vendors that "repeated violations of the rules may result in 'permanent suspension,'" and ultimately terminated hundreds of vendors. 351 F. Supp. 2d at 1103-05 & n.7. This evidence was sufficient to show that the defendant had meaningfully responded to allegations of copyright infringement and thus, "properly implemented a procedure for addressing copyright complaints and enforcing violations of its policies." *Id.* at 1103. Moreover, the plaintiff was unable to show that the defendant "could have used another, more effective and reasonable" method for preventing terminated users from re-accessing the service. *Id.* at 1103-04. Finally, addressing the "appropriate circumstances" language of the statute, the court concluded that there was insufficient evidence that the defendant had knowledge of blatant infringement – such as user statements about the pirated nature of a product, chat room discussions regarding use of the service for infringing purposes, or characteristics of listings that would give away their infringing nature – that would have required it to terminate user access. *Id.* at 1104-05. Thus, the defendant was entitled to safe harbor protection.

By contrast, the district court in *In re Aimster* confronted a policy similar to the one at issue here that warned users not to post infringing content and promised to terminate users who repeatedly violated copyright law. The court discounted the policy as an "absolute mirage" after evidence showed that the defendants obstructed ways of determining which users were transferring infringing files and, in practice, failed to terminate a single user. *In re Aimster*, 252 F. Supp. 2d at 658-59 & n.18 (declining safe

harbor protection on motion for preliminary injunction). Affirming the district court on appeal, the Seventh Circuit instructed that a "service provider must do what it can reasonably be asked to do to prevent the use of its services by 'repeat infringers.'" *Id.* at 655 (citation omitted). In a similar vein, other courts have held that "where a service provider is given sufficient evidence to create actual knowledge of blatant, repeat infringement by particular users, particularly infringement of a willful and commercial nature," it is compelled to act. *Cybernet Ventures, Inc.*, 213 F. Supp. 2d at 1176 (citing legislative history). Still others have held that there are circumstances in which operators must go beyond merely posting a policy in a site's terms of use, as Hotfile did. *See Arista Records LLC v. Usenet.com, Inc.*, 633 F. Supp. 2d 124, 131 (S.D.N.Y. 2009).[15]

Here, the scale of activity – the notices of infringement and complaints from copyright holders – indicated to Hotfile that a substantial number of blatant repeat infringers made the system a conduit for infringing activity. Yet Hotfile did not act on receipt of DMCA notices and failed to devise any actual policy of dealing with those offenders, even if it publicly asserted otherwise. It has presented no evidence to show

---

[15] The Court also notes that most of the "robust" steps Hotfile claims to have taken to prevent repeat infringement relate to its handling of particular files and not their users. Hotfile's SRA program is legally insufficient because, by its plain language, Section 512(i) requires user termination, thereby targeting future infringement from an individual who is deemed likely to recidivate. *See Cybernet Ventures, Inc.*, 213 F. Supp. 2d at 1176 ("[S]ection 512(i) is focused on infringing users, whereas 512(c) is focused primarily on the infringing material itself."). More particularly, while Section 512(c) requires service providers to remove infringing material, Section 512(i) targets the source of that infringement. *See id.* ("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." (citation omitted)).

that the small number of removals that did occur were for any reason other than threatened litigation or by court order. Indeed, it has been unable to point to a single specific user who was terminated pursuant to its policy of manual review and exercise of "discretion." Documents and statistics indicate that there was never any realistic threat of termination to Hotfile's users, whose activities were protected by the company's indifference to infringement notices. In sum, regardless of official policies forbidding infringement, Hotfile did not significantly address the problem of repeat infringers. This renders Hotfile's policy legally insufficient under Section 512(i).

Before leaving the issue, the Court briefly addresses two other points made by Hotfile. First, Hotfile contends that the Studios should be equitably estopped from asserting a DMCA challenge because of the parties' previous cooperation on infringement issues. In particular, they assert that Warner's participation in Hotfile's SRA program precludes the Studios' DMCA argument (although it should be noted that not every Studio Plaintiff participated in the SRA program.) [redacted] (Titov Decl. Ex. 31 (DE 275-10 (filed under seal); DE 321-31; DE 321-32; DE 321-33).) That individual later testified, however, that he was merely "being polite" and did not condone Hotfile's actions.

Principles of estoppel apply to copyright actions in the same manner as they apply to other actions at law. Although the parties have not cited authority discussing a

DMCA defense in particular, a copyright claim can be waived if "(1) the plaintiff [knows] the facts of the defendant's infringing conduct; (2) the plaintiff [intends] that its conduct shall be acted on or must so act that the defendant has a right to believe that it is so intended; (3) the defendant [is] ignorant of the true facts; and (4) the defendant [relies] on the plaintiff's conduct to its injury." *Carson v. Dynegy, Inc.*, 344 F.3d 446, 453 (5th Cir. 2003) (collecting authority). Here, although Hotfile has pointed to an isolated discussion that may be useful in a cross-examination at trial, there are no facts to sustain a conclusion that the Studios have acquiesced to Hotfile's conduct. The Studios appear to have protected the rights to their content, and there is no suggestion that they knew and approved of the extent of Hotfile's actions (or inaction).

Second, Hotfile has moved for partial summary judgment on the applicability of the DMCA to conduct that occurred after this litigation was initiated. As support, Hotfile provides evidence of a continuum of increased compliance, such as applying new fingerprinting and hashing technology, giving copyright owners access to Hotfile's SRA program, and implementing other "powerful countermeasures," spanning from the summer of 2009 through Hotfile's retooling of its affiliate program in February 2012, a year after this litigation began. Some of this evidence shows that Hotfile took meaningful, recent steps to combat infringement. For example, it is undisputed that Hotfile adopted and began to implement a three-strikes policy, resulting in the termination of over 20,000 of its users after the start of this litigation. Although the Court is mindful that the DMCA does not specify the characteristics of a reasonably implemented policy, it is unaware of any situation in which a three-strikes policy has been found to be ineffective. *See, e.g., Viacom Int'l Inc. v. YouTube, Inc.*, 718 F. Supp.

2d 514, 528-29 (S.D.N.Y. 2010) *rev'd in part on other grounds*, 676 F.3d 19 (2d Cir. 2012) (discussing strike-based policies).

This request to limit liability raises questions of whether a party can ever regain the protections of the DMCA and whether the Court should trust Hotfile not to revert to their offending conduct; whether the Court can determine the exact point at which Hotfile implemented a DMCA-compliant policy and, if so, whether the Court should use the date of technical compliance as the point of entry to safe harbor or whether the proper measure should be when Hotfile ceased to be a hotbed for infringement (since many DMCA requirements have a prospective purpose); and whether the parties have conducted a sufficient amount of discovery for the Court to make these determinations at this stage. However, in their briefing and at a day-long oral argument, the Studios made clear that they have brought suit based on Hotfile's system and business model "as they existed pre-Complaint" and that post-Complaint damages are not a part of this dispute. Accordingly, relying on these express representations and because the Studios have not yet made any claim concerning post-Complaint damage, the Court need not decide these issues and refrains from issuing an advisory opinion on Hotfile's current practices.

2. Other Disqualifying Factors

Having concluded that a necessary precondition to DMCA safe harbor eligibility – a reasonably implemented repeat infringer policy – is lacking as a matter of law, the Court concludes that Hotfile's DMCA defense fails. Nevertheless, the Court offers observations and conclusions about two of the remaining DMCA requirements.

a. DMCA Agent

Section 512(c)(2) requires that a service provider "designate[ ] an agent to receive notifications of claimed infringement . . . by making available through its service, including on its website in a location accessible to the public, and by providing to the Copyright Office, substantially the following information: (A) the name, address, phone number, and electronic mail address of the agent." 17 U.S.C. § 512(c)(2). Per the express terms of the statute, "[o]nly substantial compliance with the enumerated requirements is required by subsection 512(c)(2), as is also the case with subsection (c)(3)." *Perfect 10, Inc. v. Amazon.com, Inc.*, No. CV 05-4753 AHM (SHx), 2009 WL 1334364, at *8 (C.D. Cal. May 12, 2009) (citing H.R. Rep. No. 105-551(II) (1998)). The legislative history for the provision includes the following committee statement, which explains that decision:

> The Committee intends that the substantial compliance standard in subsections (c)(2) and (c)(3) be applied so that technical errors (such as misspelling a name, supplying an outdated area code if the phone number is accompanied by an accurate address, or supplying an outdated name if accompanied by an e-mail address that remains valid for the successor of the prior designated agent or agent of a copyright owner) do not disqualify service providers and copyright owners from the protections afforded under subsection (c). The Committee expects that the *parties will comply with the functional requirements of the notification provisions–such as providing sufficient information so that a designated agent or the complaining party submitting a notification may be contacted efficiently*–in order to ensure that the notification and take down procedures set forth in this subsection operate smoothly.

S. Rep. No. 105-190 (1998) (emphasis added). "To prevail at trial, the service provider has the burden of proving that it properly designated a copyright agent and that it responded to notifications as required." *Perfect 10, Inc.*, 2009 WL 1334364, at *8.

Here, the record shows that Hotfile had a "report abuse" form on its website and provided an e-mail address where users could report infringing content. It did not register a DMCA agent with the Copyright Office until December 2009; did not identify an agent on its website until May 2010; and, to date, has not provided a proper mailing address for its registered agent insofar as it lists only a post office box. *See* 37 C.F.R. § 201.38(c) (noting that the submission of an agent designation must bear the caption "Interim Designation of Agent to Receive Notification of Claimed Infringement" and include, among other things, a "full address" and not a "post office box or similar designation . . . except where it is the only address that can be used in that geographic location"). While the statute focuses on whether someone with an infringement complaint would be able to contact the company, courts have held that substantial compliance in the DMCA context "means substantial compliance with all its clauses, not just some of them." *Perfect 10, Inc. v. Yandex N.V.*, No. C 12-01521 WHA, 2013 WL 1899851, at *3 (N.D. Cal. May 7, 2013) (discussing 17 U.S.C. § 512(c)(3)). Thus, even were Hotfile otherwise able to avail itself of the DMCA safe harbor, the Court concludes that it would be ineligible under Section 512(c)(2) at least through May 2010, the date on which it published its agent's contact information. *See Yandex*, 2013 WL 1899851, at *7 ("The phrase 'substantially all the following information' modifies the ensuing the subparagraphs that list types of contact information . . . it cannot excuse a failure to provide the Copyright Office with any information at all.").

b. Actual or Red Flag Knowledge of Infringement

Finally, much of the Studios' briefing addresses Section 512(c)(1)(A)(i), which requires that a defendant not have "actual knowledge that the material or an activity

using the material on the system or network is infringing" without removing it. 17 U.S.C. § 512(c)(1)(A)(i). The safe harbor also requires that the defendant not have knowledge "of facts or circumstances from which the infringing activity is apparent." 17 U.S.C. § 512(c)(1)(A)(ii). As one court interpreting the statute explained, "[t]he 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." *ALS Scan, Inc.*, 239 F.3d at 625. These provisions of the DMCA are designed to "deny safe harbor protection to Internet service providers operating or linking to pirate sites whose illegal purpose is obvious to a reasonable person." *MP3tunes, LLC*, 821 F. Supp. 2d at 643-44 (citing S. Rep. No. 105-190 (1998)).

Nevertheless, there are two important limitations on disqualification. First, Section 512(m) specifies that a service provider has no duty to monitor activity occurring on its service or to "affirmatively seek facts indicating infringing activity," which informs the knowledge analysis. 17 U.S.C. § 512(m). Second, because the statute elsewhere imposes the requirement that providers remove every piece of material identified as infringing, "[g]eneral awareness of rampant infringement is not enough to disqualify a service provider of protection." *MP3tunes, LLC*, 821 F. Supp. 2d at 644. Instead, the section "requires knowledge or awareness of specific infringing activity." *Viacom Int'l, Inc.*, 676 F.3d at 30-32 (collecting authority) ("[T]he nature of the removal obligation itself contemplates knowledge or awareness of specific infringing material, because expeditious removal is possible only if the service provider knows with particularity which items to remove."); *accord UMG Records, Inc.*, 2013 WL 1092793, at *11

(declining to adopt "a broad conception of the knowledge requirement" and holding that the safe harbor requires "specific knowledge of particular infringing activity").

Alternatively, "the red flag provision turns on whether the provider was *subjectively* aware of facts that would have made the specific infringement 'objectively' obvious to a reasonable person." *Viacom Int'l, Inc.*, 676 F.3d at 31 (emphasis added). Courts have recognized that while willful blindness under the common law – i.e., an intentional effort to avoid guilty knowledge – can equate to actual knowledge, a DMCA analysis should not lose sight of the focus on specificity. *Id.* at 35 ("[W]illfull blindness [ ] may be applied, in appropriate circumstances, to demonstrate knowledge or awareness of specific instances of infringement under the DMCA."); *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93, 107, 109-10 (2d Cir. 2010). In a recent decision analyzing the competing considerations of the statute, one court concluded that a lack-of-knowledge defense was a triable issue because several documents in the record could have been viewed "as imposing a duty to make further inquiries into 'specific and identifiable' instances of possible infringement." *Capitol Records, Inc. v. MP3tunes, LLC*, No. 07 Civ. 9931 (WHP), 2013 WL 1987225, at *3 (S.D.N.Y. May 14, 2013) (citation omitted).

With regard to Hotfile's actual knowledge, the Studios' proof consists primarily of circumstantial evidence of infringement. The Studios assert that Hotfile does not serve a primarily lawful purpose, citing the facts that Hotfile pays users based on downloads rather than uploads (suggesting that it is a file sharing, rather than storage, service) and that a high percentage of downloaded files are infringing (suggesting infringing files are the most popular and drive user activity). The Studios thus contend that Hotfile resembles other peer-to-peer file sharing networks that have been shut down,

highlighted by the fact that Hotfile's business increased as some of those systems became inactive. As further support, the Studios cite documents containing purported admissions that Hotfile is "the flagship of non-licensed content."

In response, Hotfile states that it provides a vehicle for the distribution of files with the authorization of the content owner and that the primary purposes of its system are personal storage, "space shifting" and distribution of non-protected materials. Indeed, Hotfile has shown that one of the Studios used Hotfile to distribute its own content. And Hotfile points to statistics showing that its network is actually used for those purposes, observing that most files have never been downloaded (i.e., most uploaded files have not been retrieved by another user); that the most popular links currently available are for noninfringing content (such as open-source software) that is meant to be freely copied and shared; that there is no search feature that allows users to locate files; and that only a small percentage of files have been the subject of a DMCA notice or SRA action or have been the subject of infringement. According to Hotfile, it is a small business trying to eke out a reasonable profit in a prohibitively litigious world.

Considering all of the evidence, the Court cannot say – and does not need to determine – which Hotfile is before it. The testimony, documents and evidence of particular system characteristics create an issue of fact for a jury as to whether Hotfile knew or blinded itself to actual infringement of particular works, on a small or large scale. The master copy policy as it existed prior to this litigation, for instance, could mean that Hotfile was attuned to the infringing nature of files, but merely disabled the offending link rather than removing the file itself. Because a significant number of the

DMCA notices concerned the Studios' works, a jury could conclude that Hotfile understood that it was continuing to make particular infringing content available to the public or that, at the very least, it should have investigated those files. Similarly, to the extent that communications with users should have alerted Hotfile to the infringing nature of files on its system that were owned by the Studios (such as users seeking technical assistance who indicated that their difficulties were owing to the illegal nature of their activity), Hotfile might be deemed to have possessed red flag knowledge. *See UMG Recordings, Inc.*, 2013 WL 1092793, at *14 (stating that had e-mails identifying infringing content come from a system's users, rather than the copyright owner, "it might meet the red flag test because it specified particular infringing material"). Indeed, based on the evidence put on by the parties, a jury might even determine that Hotfile should have understood that particular material was infringing (or at least should have looked into whether infringement was occurring) when it became aware of the link name.

But "[a]s a general rule, a party's state of mind (such as knowledge or intent) is a question of fact for the factfinder, to be determined after trial." *Chanel, Inc. v. Italian Activewear of Fla., Inc.*, 931 F.2d 1474, 1476 (11th Cir. 1991). Thus, as to actual or red flag knowledge of infringement, the Court concludes that a genuine issue of material fact exists, and this issue would have to be resolved by a jury at trial.

B. Liability for Infringement

Without the benefit of the DMCA safe harbor, the Court must still determine whether Hotfile is liable for the copyright violations committed by its users. The DMCA does not supplant common law principles of liability, and a finding that such a protection is unavailable does not necessarily mean that liability for infringement on the system is

proper. *See Columbia Pictures Indus., Inc. v. Fung*, 710 F.3d 1020, 1039-40 (9th Cir. 2013) ("[W]e are not clairvoyant enough to be sure that there are no instances in which a defendant otherwise liable for contributory copyright infringement could meet the prerequisites for one or more of the DMCA safe harbors. We therefore think it best to conduct the two inquiries independently – although, as will appear, aspects of the inducing behavior that give rise to liability are relevant to the operation of some of the DMCA safe harbors and can, in some circumstances, preclude their application."); *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1174 (C.D. Cal. 2002) ("These 'safe harbors' do not affect the question of ultimate liability under the various doctrines of direct, vicarious, and contributory liability . . . Rather they limit the relief available against service providers that fall within these safe harbors."); *cf. Flava Works, Inc.*, 689 F.3d at 758 ("[A] noninfringer doesn't need a safe harbor.").

Courts have struggled with defining the liability of Internet-based companies that provide the technological mechanism to foster, or at least enable, others to infringe. This confusion and uncertainty prompted in part the enactment of the DMCA. *See, e.g., Sony Corp. of Am. v. Universal City Studios*, 464 U.S. 417, 434 n.17 (1984) ("*Sony/Betamax*") (noting that "the lines between direct infringement, contributory infringement, and vicarious liability are not clearly drawn" (quoting district court decision)); *Flava Works, Inc.*, 689 F.3d at 760 ("The only distinctions relevant to this case are between direct infringement . . . and contributory infringement, and between contributory infringement and noninfringement.").

Even so, courts have recognized the value and remaining viability of a claim of secondary liability: "When a widely shared service or product is used to commit

infringement, it may be impossible to enforce rights in the protected work effectively against all direct infringers, the only practical alternative being to go against the distributor of the copying device for secondary liability on a theory of contributory or vicarious infringement." *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913, 929-30 (2005) (citation omitted); *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1171 n.11 (9th Cir. 2007) ("[C]opyright holders cannot protect their rights in a meaningful way unless they can hold providers of such services or products accountable for their actions.") These theories of secondary liability – contributory infringement, inducement liability and vicarious liability – are court-created and do not rely on the Copyright Act or another statute. *See Viacom Int'l Inc.*, 676 F.3d at 28 n.5 (citing *Grokster*, 545 U.S. at 930-31); *Perfect 10, Inc. v. Visa Int'l Serv. Ass'n*, 494 F.3d 788, 795 (9th Cir. 2007) ("Contributory copyright infringement is a form of secondary liability with roots in the tort-law concepts of enterprise liability and imputed intent.").

1. Inducement and Contributory Infringement

The Supreme Court's seminal 2005 decision in *Grokster* observed that "[o]ne infringes contributorily by intentionally inducing or encouraging direct infringement." 545 U.S. at 929. "[C]ontributory liability is based on the defendant's failure to stop its own actions which facilitate third-party infringement." *Amazon.com, Inc.*, 508 F.3d at 1175. The theory has two requirements: (1) the defendant knows of direct infringement, and (2) the defendant "induces, causes, or materially contributes to [that] infringing conduct." *Napster, Inc.*, 239 F.3d at 1020 (internal quotation and citations omitted). To "establish inducement liability, it is crucial to establish that the distributors communicated an

inducing message to their . . . users.'" *Visa Int'l Serv. Ass'n*, 494 F.3d at 801 (internal quotation omitted).

Thus, to establish this derivative liability, a plaintiff must first make a prima facie case of direct infringement by a third party, which is done by proving ownership of a particular work and evidence of unauthorized copying. *Napster, Inc.*, 239 F.3d at 1013 n.2; *Situation Mgmt. Sys., Inc. v. ASP Consulting LLC*, 560 F.3d 53, 58 (1st Cir. 2009) (quoting *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 361 (1991)). In this case, the parties do not dispute that the Studios own 3,800 works at issue and that they have properly registered them under Section 411 of the Copyright Act. Moreover, while Hotfile takes issue with the Studios' method for proving infringement, it does not dispute that at least some of the Studios' works have been illegally copied or downloaded using the Hotfile system. This has caused the Studios to lose money they would have earned from licensing the content to users and because of the threat of further downstream "viral" distributions. The Waterman study and the facts of the counterclaim provide competent proof in that regard; any other questions merely go to the level of damages. *Cf. Fung*, 710 F.3d at 1034.

The more vexing question here concerns the hallmark of this type of liability – whether intent can be expressly shown or inferred from Hotfile's actions. The Studios allege that infringement is a natural consequence of Hotfile's business model; that the company "actively fosters" massive copyright infringement to increase its revenue; and that despite storing all infringing content on its servers, it failed to mitigate infringement.

a. *Grokster*-type Intent

In this regard, courts have held that even though an entity merely distributes a device that causes infringement, it may nonetheless be liable for inducement if the defendant has "the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement." *Grokster*, 545 U.S. at 919. Liability may be imposed "if the actor knowingly takes steps that are substantially certain to result in [ ] direct infringement." *Amazon.com, Inc.*, 508 F.3d at 1170. Or, a defendant can encourage or induce infringement through certain acts, "such as advertising an infringing use or instructing how to engage in an infringing use." *Grokster*, 545 U.S. at 936 (citations and internal quotations omitted). In addition to these methods of directly proving intent, an actor may be liable under older common law theories based on imputing intent, such as by knowing of specific acts of infringement and failing to act or by providing "material support" to those who commit infringement. As discussed below, there is disagreement as to the parameters of these doctrines, whether they continue to apply, and what defenses may be applicable to counter the deleterious effect they may have on innovation and the benefits of technology.

The decision in *Grokster* illustrates what unquestionably suffices to show actual intent. There, a group of copyright holders consisting of recording companies, songwriters and music publishers sued companies that distributed software products enabling peer-to-peer file sharing among users. 545 U.S. at 919. The defendants did not maintain copies of files on their servers, did not know which files their users were transmitting, and did not effectively control user-behavior. *Id.* at 920 & n.1, 922. But evidence showed that "the probable scope of copyright infringement is staggering" and

that the defendants were aware of the nature of the infringement. *Id.* at 923. Similar to the facts of this case, an expert commissioned by one of the plaintiffs concluded that 90 percent of the files on one of the systems were infringing, although the defendants raised methodological challenges, suggested that the software had significant noninfringing uses, and provided other "anecdotal and statistical evidence" to show that files might not have been copyright protected. *Id.* at 922-23. Finally, e-mails from users "with questions about playing copyrighted movies they had downloaded" and notifications from one of the plaintiffs about the infringing nature of certain files demonstrated the defendants' knowledge of the fact of infringement. *Id.* at 923.

The Court went beyond knowledge of infringement, however, to address actual evidence of intent. It concluded that the defendants "clearly voiced the objective that recipients use it to download copyrighted works, and each took active steps to encourage infringement." *Id.* at 923-24. In particular, one of the defendants designed and advertised software to compete with a system that was ruled to have been infringing (Napster), thereby "aiming to satisfy a known source of demand for copyright infringement." *Id.* at 924, 939. Their business models were centered on advertising revenue driven by the popularity of content, which the court equated with infringing content and which confirmed "that [defendants'] principal object was use of their software to download copyrighted works." *Id.* at 926 ("Users seeking Top 40 songs, for example, or the latest release by Modest Mouse, are certain to be far more numerous than those seeking a free Decameron, and Grokster and StreamCast translated that

demand into dollars.")[16] Finally, the Court found that companies failed to develop tools "to diminish the infringing activity [of] using their software," thereby underscoring their "intentional facilitation of their users' infringement." *Id.* at 939.

After discussing the plaintiffs' prima facie case of liability for inducement and vicarious liability, which fall under the umbrella of secondary liability, the *Grokster* Court considered defenses. In particular, it discussed its holding in *Sony/Betamax*, which the court of appeals had applied in affirming the district court's grant of summary judgment.[17] That decision applied the "staple article of commerce doctrine" and concluded that an actor distributing a commercial product (such as a video recording device) is not liable for acts of infringement, even if it knows of actual or likely infringement, unless the product is incapable of substantial noninfringing uses. *Grokster*, 545 U.S. at 932-333 (discussing the holding of *Sony/Betamax*). The Court sought to balance the harms that infringement has on copyright owners with the effect liability might have in stifling commerce and innovation. Thus, it suggested that the doctrine applies only to circumstances where no intent to promote infringing uses can be imputed from the design of a distributed product and where the defendant has not "expressed an object" of bringing about infringement, such as by advertising uses that

---

16 This was contrary to the district court's conclusion that the defendants were entitled to summary judgment and its reasoning that distributing the software "did not provide the distributors with actual knowledge of specific acts of infringement." *Id.* at 927 (citing district court decision).

17 Similar to the appellate court's holding, prior precedent in the Eleventh Circuit concluded that *Sony/Betamax* applies to all forms of contributory liability. *Cable/Home Comm'n Corp. v. Network Prods., Inc.*, 902 F.2d 829, 845 (11th Cir. 1990) ("Contributory infringement will not be found if the product in question is capable of 'substantial noninfringing uses,' the determinative issue in *Sony,* and clarified in that case as wide use 'for legitimate, unobjectionable purposes.'" (quoting *Sony/Betamax*, 464 U.S. at 442)).

are necessarily infringing. *Id.* at 933. In other words, the *Sony/Betamax* rule does not bar liability where a plaintiff pleads an inducement theory of secondary liability premised on actual evidence of intent. *Id.* at 933 ("*Sony* barred secondary liability based on presuming or imputing intent to cause infringement solely from the design or distribution of a product capable of substantial lawful use, which the distributor knows is in fact used for infringement. . . . Because *Sony* did not displace other theories of secondary liability, and because we find below that it was error to grant summary judgment to the companies on MGM's inducement claim, we do not revisit *Sony* further.").

The *Grokster* Court concluded that "one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties," and, in that instance, the staple article of commerce doctrine does not act as an affirmative defense. *Id.* at 936-37. A showing of intent requires evidence of active steps taken to entice or persuade another to infringe and cannot be established from "mere knowledge of infringing potential," "actual infringing uses," "a failure to take affirmative steps to prevent infringement," or "ordinary acts incident to product distribution, such as offering customers technical support or product updates." *Id.* at 935-37, 939 n.12, 940 (stating that the fact that a business model benefits from infringement could not alone "justify an inference of unlawful intent, but viewed in the context of the entire record its import is clear"). Instead, liability must be premised on "purposeful, culpable expression and conduct." *Id.* at 937.

Based on the evidence presented, the Court in *Grokster* found an "unlawful objective" that was "unmistakeable": the system was used predominately to infringe.

The Court predicated its conclusion on the facts that the defendants learned of the infringing nature of use when providing technical assistance; the business competed with another system whose users were known to have infringed; the business model was driven by the availability of unlicensed content; and the defendants took no meaningful steps to prevent infringement.[18] *Id.* at 941.

b. Material Contribution Liability

Developing guidance for some of *Grokster*'s unanswered questions, a more recent case from the Southern District of New York reviewed the file sharing service LimeWire and addressed how the legal theories of inducement of infringement, contributory infringement, common law infringement and unfair competition fit together. *Lime Group*, 784 F. Supp. 2d at 409. The service at issue employed peer-to-peer technology through which software created by the defendants took an inventory of files on users' computers and allowed others to search for and download them directly. *Id.* at 410-411. The same expert engaged by the Studios in this case, Dr. Waterman, concluded that 98.8 percent of the files downloaded through LimeWire were not authorized for free distribution and that 43.6 percent of those files were owned by the plaintiffs in the action. *Id.* at 412. The court determined that there was sufficient evidence of direct infringement by LimeWire users and that the Waterman report provided competent proof of the scope of that infringement. *Id.* at 422-24.

On the issue of *Grokster*-type inducement, the court found that summary judgment in favor of the plaintiffs was warranted. *Id.* at 426. Evidence cited by the

---

[18] Ultimately, on remand, the district court entered summary judgment in favor of the plaintiffs on the issue of liability. *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 454 F. Supp. 2d 966, 999 (C.D. Cal. 2006).

court to establish the defendants' awareness of infringement included: (1) the scope of the infringement, which revealed that "most actual downloads involve unauthorized content;" (2) internal communications that not only noted that users were sharing digital recordings, but also acknowledged that they were copyrighted (including a document in which the defendants considered legitimizing and monetizing user activity); (3) the fact that the infringing nature of the activity was communicated to defendants through user e-mails and the company maintained articles about infringement in a file labeled "Knowledge of Infringement;" and (4) the fact that the defendants provided technological assistance with files that "plainly relate[d] to unauthorized sharing of digital recordings." *Id.* at 426-28.

Moreover, like the network in *Grokster*, the defendants developed business strategies to target users of shuttered networks; their advertisements intimated illegal uses; and their revenue relied on the popularity of content that was indirectly tied to infringement. *Id.* at 427-29. Other attributes of the LimeWire software suggested that it was designed with infringement in mind. The program not only enabled searches, but also suggested popular and copyrighted recordings to users; the defendants even tested its functionality using protected titles. *Id.* at 428. Moreover, the defendants failed to implement any sort of technical barrier or design choice to diminish infringement; instead, while existing technology could have been applied to infringing works, that filtering technology was disabled by default (and had to be enabled by users). *Id.* at 429-430. Finally, the defendants had considered alternative business models, including opening a store to guide users to licensed content. *Id.* This evidence was sufficient to show the same kind of unmistakeable intent as existed in *Grokster*.

But in addressing other common law principles of secondary infringement, Judge Wood concluded that summary judgment was inappropriate. The decision made a distinction between inducement liability, which requires *Grokster*-type evidence of intent, and contributory infringement liability, which does not so long as a defendant's contribution to infringing activities is "material." [19] *Id.* at 432. Under the contributory infringement theory of liability, the court found that the evidence was sufficient to show the defendants' knowledge of and material contribution to substantial infringing activity. *Id.* at 434. However, applying the *Sony/Betamax* rule, the court found there was insufficient evidence that the LimeWire service was incapable of substantial noninfringing uses. *Id.* The court observed that, while the LimeWire service was used "overwhelmingly for infringement" at the time of the decision, the defendants demonstrated substantial noninfringing uses that existed or were likely to develop,

---

[19] The decision reasoned that *Grokster* answered the question of inducement liability but failed to determine "whether the Ninth Circuit had been correct in granting summary judgment on the contributory infringement claim." *Id.* at 433. The concurring opinions in *Grokster* debated whether the noninfringing uses identified by the defendants were sufficient to merit summary judgment, but agreed that the *Sony/Betamax* rule continues to act as a defense to contributory infringement. *Id.* at 433 (citing concurring opinions); *see also* Alfred C. Yen, *Torts and the Construction of Inducement and Contributory Liability in Amazon and Visa*, 32 Colum J.L. & Arts 513, 513 (2009) ("In [*Grokster*], the Supreme Court adopted intentional inducement as a cause of action for third party copyright liability. Before *Grokster*, such liability existed in two forms, contributory liability and vicarious liability . . . Now, after *Grokster*, a defendant also faces liability if she acts with the object of promoting infringement by others." (footnote omitted)). Other decisions have suggested that two categories of contributory infringement liability exist – "actively encouraging (or inducing infringement through specific acts . . . or [ ] distributing a product distributees use to infringe copyrights, if the product is not capable of 'substantial' or 'commercially significant' noninfringing uses" – and that *Sony/Betamax* serves as a defense where the latter is asserted. *Amazon.com, Inc.*, 508 F.3d at 1170 (quoting *Grokster*, 545 U.S. at 942 (Ginsburg, J., concurring)).

including distribution of non-protected works. *Id.* Thus, under the *Lime Group* analysis, the *Sony/Betamax* rule may still be raised as a theory of defense where the intent to infringe or induce infringement is not explicit, but rather is imputed from a defendant's material contribution to infringement.

Several other courts have considered the material contribution theory of liability but have not always addressed the applicability of the *Sony/Betamax* defense under that theory. In *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259 (9th Cir. 1996), operators of a swap meet where counterfeit goods were sold were deemed to have provided the "support services" for infringement, including "the provision of space, utilities, parking, advertising, plumbing, and customers," such that the swap meet operators could be held liable. *Id.* at 263. Extending that theory of liability to the Internet context, the district court in *Napster* found the search and directory features of the music sharing program to be "an Internet swap meet." *A&M Records, Inc. v. Napster, Inc.*, 114 F. Supp. 2d 896, 919-20 (N.D. Cal. 2000) (quoting briefing), *aff'd in part & rev'd in part*, 239 F.3d 1004, 1022 (9th Cir. 2001). On appeal, albeit in a pre-*Grokster* decision, the Ninth Circuit found that the *Sony/Betamax* defense was applicable to instances in which intent to promote infringement was imputed from the structure of the system, but inapplicable to instances where the defendant has identified specific information regarding infringing activity. *Napster*, 239 F.3d at 1020-22. While the court concluded that the defendants were also liable under a *Fonovisa* material contribution theory, it did not address whether the *Sony/Betamax* defense applies under that theory. *Id.* at 1022.

In *In re Aimster*, "[i]nstead of parking spaces, advertisements, and plumbing," the defendants "provided the software and the support services necessary for individual Aimster users to connect with each other . . . manag[ing[to do everything but actually steal the music off the store shelf and hand it to Aimster users." 252 F. Supp. 2d at 659. The court disallowed the *Sony/Betamax* defense, reasoning that the online network had an ongoing relationship with the direct infringer, as opposed to merely providing the means to commit infringement in a single point-of-sale transaction, like selling a VCR – an argument aggressively pursued by the Studios in this case.[20] Moreover, the Aimster technology permitted mass distribution of infringing content rather than "private, home use copying." *Id.* at 653. Rather than focusing solely on the features of the staple article of commerce doctrine, the decision made a distinction that would be echoed three years later in *Grokster* : there was both a lack of evidence that the technology had legitimate purposes and significant evidence that the defendant intended to foster infringement. *Id.* at 652-64.

For the most part, as in *Lime Group*, recent decisions have suggested that the *Sony/Betamax* rule applies wherever material contribution is at issue. *See, e.g., Capitol Records, LLC v. ReDigi Inc.*, No. 12 Civ. 95 (RJS), 2013 WL 1286134, at *13 (S.D.N.Y. Mar. 30, 2013) ("However, even where a defendant's contribution is material, it may evade liability if its product is 'capable of substantial noninfringing uses.'" (quoting *Sony/Betamax*, 464 U.S. at 442)).

---

[20] While other courts have used this distinction to decline to apply the *Sony/Betamax* rule, this Court includes the analysis of an ongoing relationship in the vicarious liability context. As explained below, that theory of liability examines a defendant's relationship with, and control over, direct infringers to hold the defendant liable, just as a principal may be liable for the actions of his agent.

c. Knowledge of Infringing Content and Failure to Remove

Finally, the Ninth Circuit's decision in *Perfect 10, Inc. v. Amazon.com, Inc.* shows that the *Grokster* decision does not foreclose other common law principles of imputing intent. In particular, a provider may face liability where it knows of particular instances of infringement – rather than simply that the system is capable of infringement or generally permits some level of infringement – and fails to act to remove it. There, a copyright owner sued two companies, one of which (Google) operated a search engine that permitted users to search the Internet for images and facilitated downloads of those images from third-party websites by linking to them. 508 F.3d at 1155-56. On the issue of secondary infringement, it was undisputed that the third parties did not have permission to display plaintiff's images on their websites and that some direct infringement had occurred. *Id.* at 1169.

The parties disagreed, however, as to whether Google fostered infringement through specific acts under *Grokster*. Although there was no suggestion that Google actually induced copyright infringement, the Ninth Circuit applied common law tort principles of fault-based liability to reason that "an actor may be contributorily liable for intentionally encouraging direct infringement if the actor knowingly takes steps that are substantially certain to result in direct infringement." *Id.* at 1170-71 & n.11. It also relied on its pre-*Grokster* decision in *Napster*, which held that "if a computer system operator learns of specific infringing material on his system and fails to purge such material from the system, the operator knows of and contributes to direct infringement" under a material contribution theory. *Id.* at 1171. The court was persuaded by the reasoning that secondary infringement should be available to provide a practical mechanism for

preventing direct infringement. *Id.* at 1172. Because the district court had applied a different standard and there was evidence that "Google substantially assist[ed] websites to distribute [users'] infringing copies to a worldwide market and assist[ed] a worldwide audience of users to access infringing materials," Google could have been liable if it failed to take simple measures to prevent damage to the plaintiff. *Id.*[21]

d. Application of Precedent

Against this body of jurisprudence, the Court sets out the standard for inducement and contributory infringement liability it applies here. First, while it may be unclear whether *Grokster* introduced a new category of liability based on inducement or whether it spoke to pre-existing notions of contributory liability, it is evident that a defendant will be liable for actually expressing an intention to foster infringement. If that intent is express or can otherwise be said to be "unmistakeable," the *Sony/Betamax* defense will not apply and the defendant will be liable for all acts of direct infringement committed using its system, as was the case in *Grokster*. Similarly, as explained in *Amazon.com*, where traditional principles permit a court to impute intent – for instance, where the defendant knows of specific infringing content available on its system yet fails to remove it – that defendant may be liable, by operation of law, just as if he had actually intended to infringe under *Grokster*. Finally, contributory infringement may be

---

[21] On remand, the district court rejected the plaintiff's request for a preliminary injunction because the plaintiff failed to show that individual notices of infringement that had elicited no response were adequate to confer knowledge of infringement on Google. *Perfect 10, Inc. v. Google, Inc.*, No. CV 04-9484 AHM (SHx), 2010 WL 9479060, at *6-7 (C.D. Cal. July 30, 2010). Plaintiff also failed to show that practical and simple measures to prevent infringement were available to Google as a viable remedy. *Id.* at *7. Nor could the plaintiff meet the other requirements for a preliminary injunction. *Id.* at *14. The decision was affirmed, 653 F.3d 976 (9th Cir. 2011), and certiorari was denied by the Supreme Court, 132 S.Ct. 1713 (Mar. 5, 2012).

found based on a material contribution theory in instances where a defendant did not express an intention to foster infringement but provided the means for infringement or distributed a commercial product that was subsequently used to infringe. Under that theory, the *Sony/Betamax* rule provides a backstop to liability, immunizing a defendant who demonstrates that noninfringing uses of the system are substantial. The Studios have raised claims and presented facts related to each of these theories of liability.

As a preliminary matter, it should be understood that although Hotfile has many unique characteristics, it is also true that it shares many of the attributes that have doomed other networks.[22] Most notably, the Court concludes that the extent of infringement by Hotfile's users was staggering, as was the case in *Grokster*. On this point, Hotfile questions the Waterman study and its finding of a respective 90.2% and 5.3% rate of infringement and noninfringement based on an examination of files that had been downloaded. The Court agrees that the study assumed an infringing purpose and that an examination of *uploaded* files – including those that were never shared or downloaded – would likely have shown a lower infringement rate and alternative uses for Hotfile's system apart from infringement (as Hotfile's expert, Dr. James Boyle, points out). It may also be true, as Hotfile argues, that the Waterman study examined too short of a time period (i.e., one month of data) and improperly excluded entire categories of files that would have resulted in an even lower rate.

Despite Hotfile's quarrel with the Waterman rate and suggestion that it is somewhat high, it cannot dispute that an enormous amount of infringement has actually

---

22 The Studios contend that Hotfile is similar to other infringing networks, such as Grokster, Fung, Streamcast, Usenet.com, and LimeWire.

occurred on Hotfile's system. For example, the record reflects a large number of DMCA notices received by Hotfile – eight million in total. As is explained in the Court's discussion of the counterclaim, only a relatively small number of the notices pertaining to Warner have been claimed to be incorrect and noninfringing, suggesting the same may be true of the other sets of notices Hotfile received from the Studios. Moreover, while the Court cannot deduce that every file posted by a repeat infringer is actually infringing, the uploads of those subject to three or more notices constituted 44 percent of all files on Hotfile (and half of all downloaded files) in February 2011. At the very least, this shows that a high number of Hotfile users likely engaged in infringement – the vast majority of Hotfile's top affiliates, and well over 20,000 of its users – and were likely responsible for a substantial amount of infringement. Indeed, the Studios have identified over 900,000 files containing their own works that were available for the taking. These numbers are consistent with the demonstrated outcome of Hotfile's post-Complaint policy changes, which Hotfile asserts were effective in combatting infringement and resulted in the termination of affiliates and users, deletion of files, and a substantial drop in revenue.

The Court can also conclude that Hotfile became aware of the general fact of infringement – although possibly not its scale – at least when it received DMCA notices through its agent and when it was sued or threatened with suit by copyright holders. Documents produced in discovery suggest that Hotfile was aware it was becoming "the flagship of non-licensed content;" that if it had examined the files on its system, it would have known of the infringing activity; and that it was doing business with those it suspected were infringers like the affiliate PlanetSuzy. Hotfile provided the means of

infringement; it created and currently maintains the Hotfile website, which Hotfile's members actually use to infringe. Users even store the infringing content on Hotfile's own servers, in contrast to decentralized peer-to-peer networks, in which the information resides on users' computers.

Finally, there is some evidence suggestive of a deliberate design to facilitate infringement. Hotfile is deliberately modeled after networks that were subsequently subject to challenges of infringement; its incentive structure rewards large and frequent file downloads; it pays members through an affiliate program; and it relies on the popularity of content to drive growth, even imploring users to post "interesting" links and media files. The fact that it actually pays infringers for this activity is, as the Studios argue in briefing, "simply unprecedented." Hotfile also provides technical assistance to those who infringe, both by answering specific questions from users about downloading media and by providing tutorials that reference copyrighted works. And, despite having the means to implement counter-piracy technologies and to target infringement (as demonstrated by Hotfile's actions immediately after the Complaint was filed), Hotfile did not take any meaningful action to curtail infringement. Moreover, it did not have an effective policy to terminate blatant, repeat infringement, which constituted a substantial amount of the total infringement, until February 2011. Based on the totality of the evidence, the Court concludes that Hotfile was successful in large part because it did not control infringement activity on its system.

Nonetheless, the Court draws distinctions between this case and the case law recited above in which courts determined that judgment on the question of secondary liability was proper. For instance, despite an increase in user traffic, the Studios have

shown neither that Hotfile's inspiration, RapidShare, actually was a pirate network nor that Hotfile targeted RapidShare's users to satisfy a known source of demand for copyright infringement, as was the situation in cases finding liability for networks attempting to become the next Napster. Indeed, as shown by the [redacted] e-mail, Hotfile apparently viewed the migration of RapidShare users as a "bad thing." (Yeh Decl. Ex. 53 (DE 288-58 (filed under seal); DE 324-11).) Moreover, Hotfile did not promote any of its files or enable a file search function, but instead relied on third-party affiliates that were responsible for promoting (and essentially making available) infringing content. All infringing activity thus took place between uploading users, downloading users and affiliates (and not Hotfile). Additionally, the system has noninfringing uses ignored in the Studios' focus on downloading activity, such as the distribution of unlicensed materials. And Hotfile eventually developed a notice and takedown system and, over time, implemented technology to combat infringing users.

Hotfile's general knowledge of infringement, even if rampant, is insufficient by itself to support liability. The Studios have not proffered an express statement by Hotfile indicating its intention to foster copyright infringement, that is, clearly voicing an objective of encouraging infringement. Not one document shows a business plan contemplating infringing uses or an understanding that Hotfile was actually assisting users (individually or as a whole) to commit infringement. Hotfile had no direct involvement in the acts of infringement (as would be the case if its employees had posted the Studios' copyrighted content). Unlike *Lime Group*, there were no considerations (and rejections) of counter-piracy software, internal communications acknowledging the illegal nature of specific network activity, or proposals to legitimize

user activity. Unlike *Grokster*, the intent to infringe is not "unmistakeable" such that it can be said to be central to the business model and ingrained in the platform's design. Indeed, Hotfile has, at least, a plausible alternative design model in the form of personal data storage.[23]

Although some evidence shows that Hotfile might have been on notice that specific acts of infringement were afoot, the evidence does not demonstrate that Hotfile knew for certain that the uses were illegal or that Hotfile induced the infringing use. For example, the Studios assert that users put Hotfile on notice that they were purchasing premium accounts "specifically to download copyrighted works." But the document supporting this assertion is an e-mail from a prospective user to a Hotfile e-mail address stating that he "wish[ed] to sign up to Hotfile to down load" eight "Ebooks" of older novels including Dickens's *A Christmas Carol*. (Yeh Decl. Ex. 66 (DE 324-12).) It is plausible that a service provider, foreign or domestic, might believe that a work from a 19th century English writer is no longer subject to copyright protection. The document shows no response from Hotfile endorsing an illegal use, and nothing about the request suggests that the user's downloads would be blatantly infringing.

The Studios also allege that Hotfile "repeatedly provided technical assistance to users they knew were seeking to download [infringing] content," such as by answering user questions when the link's URL was apparent to Hotfile. (Hotfile could see the URL path of the last file downloaded in every communication.) But Hotfile points out that it had no way of knowing whether the user lacked permission to share the file, whether

---

[23] Based on data, Dr. Boyle concluded that there were substantial noninfringing uses in the form of open source software and movie sharing, fair use downloads, storage, and monetizing works owned by creators through the affiliate program.

the file contained what the title indicated, or whether the work was actually protected by copyright. Indeed, the evidence shows that when users indicated to Hotfile that they were accessing particular content, they did nothing to conclusively inform Hotfile of the fact of infringement. While the Studios contend that by rewarding distribution of large and popular downloads (in contrast to promoting storage), Hotfile knew that it was encouraging the sharing of protected music and movies, no documents show that Hotfile equated popular content with protected content.

Thus, with respect to each example raised by the Studios, a number of questions remain regarding Hotfile's intent (actual or imputed) to foster infringement and the capacity for and scope of noninfringing uses of Hotfile's system. For example: When Hotfile supported user activity or communicated with affiliates, did it know that the files actually contained copyrighted material as the link names or discussion indicated? Did Hotfile know that the works are currently protected by copyright? Did Hotfile know when users lacked permission to download certain works (which would not have been the case if the works were user-owned and "space-shifted," or if the files were freely-licensed, as the most popular downloads on Hotfile currently are)? Was Hotfile designed, and is it primarily used, for storage or for distribution? If the latter, did Hotfile intend to promote the infringement of copyrighted work, or did it merely provide a service that was ultimately used to infringe? Did Hotfile encourage the sharing of protected content, thereby crossing the threshold from knowledge of infringement to fostering infringement? In sum, unlike other cases where the evidence of intent is more compelling, the record here does not provide an unequivocal picture. The fact that these questions remain makes summary judgment inappropriate on the theories of

inducement and contributory infringement liability. And while Hotfile may have a difficult time explaining its "innocence" to a jury,[24] the genuine issues of material fact must be resolved by a jury at trial.

2. Vicarious liability

The Studios next assert that Hotfile is vicariously liable for the actions of its users. In contrast to contributory liability, which focuses on the defendant's actions in enabling infringement, "vicarious liability is based on the defendant's failure to cause a third party to stop its directly infringing activities." *Amazon.com, Inc.*, 508 F.3d at 1175 (citations omitted). Vicarious copyright liability has been described as a variation of the doctrine *of respondeat superior* – a form of strict liability premised on agency. *See Fonovisa, Inc.*, 76 F.3d at 262. Thus, the doctrine does not require knowledge of the infringement and may be applied even where the defendant has acted in good faith to prevent it. *Id.*[25] Vicarious infringement has two elements, occurring "when one profits from direct infringement while declining to exercise a right to stop or limit it." *Luvdarts, LLC v. AT&T Mobility, LLC*, 710 F.3d 1068, 1071 (9th Cir. 2013) (citing *Grokster*, 545

---

[24] For instance, as indicated in the DMCA context, Hotfile's master file policy (which removed offending links but not the actual file) may mean that Hotfile knew of particular infringing files and failed to bar further access. Hotfile will also have to explain how, in each of these instances, it was unaware of the offending nature of the activity, did not intend to contribute to it, and could not utilize existing technology to prevent infringement. Finally, to the extent that the Studios premise liability on the fact that Hotfile provided the mechanism for infringement, Hotfile has suggested *Sony/Betamax*-type noninfringing uses for the system, and there is a question of whether those uses are "substantial."

[25] Although a defendant's lack of knowledge may not affect liability in this context, it does have implications for the measure of damages available under the Copyright Act. *See* 17 U.S.C. § 504(c)(2) (providing that statutory damages may range from $750 to $30,000 per violation, but capping willful violations at $150,000 per violation); *see also EMI April Music, Inc. v. White*, 618 F. Supp. 2d 497, 507 (E.D. Va. 2009) (citing *Nelson-Salabes, Inc. v. Morningside Dev., LLC*, 284 F.3d 505, 517 (4th Cir. 2002)).

U.S. at 930); *A&M Records, Inc.*, 239 F.3d at 1022. The determination of whether a defendant has the capacity to halt infringement is determined by examining the system's "current architecture." *Napster*, 239 F.3d at 1024.

Hotfile contends that the Studios cannot show a "direct financial benefit" from infringement because Hotfile charges a fixed rate to users through subscriptions and does not profit incrementally from infringement. Hotfile's argument rests on an early Internet case, *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995), in which a member of a religious organization posted the plaintiffs' copyrighted works to a computer bulletin board service. *Id.* at 1365-66. Those works were automatically copied to the defendant's computer by the service and thereby made available to users who paid the defendant a fixed subscription fee. *Id.* at 1365-68. The court concluded that the plaintiffs were unlikely to prevail on their vicarious liability claim because the link between infringement and revenue was not sufficiently established. *Id.* at 1376-77.

Notably, however, the *Netcom* court did not rule that a fixed fee could never provide a direct benefit basis for vicarious liability. Instead, the court observed that the plaintiffs failed to show that the policy at issue enhanced "the value of [defendant's] services to subscribers or attract[ed] new subscribers," in light of the fact that the defendant was merely an entity providing Internet access to users. *Id.* at 1377. Indeed, the only evidence of such a link consisted of a declaration from plaintiffs' counsel stating that the defendant was concerned it would lose business if an injunction were to be granted on the infringement claims. *Id.* The court found such evidence insufficient to show the type of financial tie required. *Id.*

By contrast, other courts have permitted liability where the financial benefit was even more attenuated than here. In *Arista Records LLC v. Usenet.com, Inc.*, 633 F. Supp. 2d 124 (S.D.N.Y. 2009), the court rejected an argument that causation was not established "because [the defendants] are paid on a per-volume, not per-download, basis and because infringing music accounts for less than 1% of the newsgroups available on their service." *Id.* at 157. Likewise, in the Ninth Circuit's *Napster* decision, an increase in user base – i.e., more user registrations – due to the increasing quality and quantity of available music meant that the defendants financially benefitted from infringement such that they were liable. 239 F.3d at 1023 (quoting lower court decision).

The *Napster* case posits that only a *causal* relationship between infringement and profit must be established "regardless of how substantial the benefit is in proportion to a defendant's overall profits." *Ellison v. Robertson*, 357 F.3d 1072, 1079 (9th Cir. 2004). In other words, "the law is clear that to constitute a direct financial benefit, the 'draw' of infringement need not be the primary, or even significant, draw – rather, it only need be 'a' draw." *Usenet.com, Inc.*, 633 F. Supp. 2d at 157. As one observer noted after a review of many of these cases, "[a]t present, the dominant view is that any for profit enterprise could be found vicariously liable for copyright infringement however remote, unquantifiable, and unidentifiable the benefit it receives from copyright infringement may be." Craig A. Grossman, *From Sony to Grokster, the Failure of the Copyright Doctrines of Contributory Infringement and Vicarious Liability to Resolve the War between Content and Destructive Technologies*, 53 Buff. L. Rev. 141, 230-31 (2005).

The Court has already concluded that questions remain regarding whether the financial benefit Hotfile received and the design of its business model are sufficient to impute intent to induce copyright infringement at this stage. But the vicarious liability standard requires neither that a defendant have knowledge of the acts of infringement nor that the defendant receive *substantial* financial benefit from infringement. Hotfile concedes that infringement did occur on its system and, while it argues that its support for infringement would not have made business sense, it acknowledges that infringing files drove some amount of sales to Hotfile, as shown by the Zebrak classifications and Waterman calculations. The infringement-sales connection is also indicated by the dramatic drop in Hotfile's income after the Complaint was filed and after Hotfile implemented its three-strikes policy and technologies to ferret out infringers. (*See, e.g.,* Yeh Decl. Ex. 70 (DE 288-82 (filed under seal); DE 324-13).) Hotfile may contend that infringement was not central to its success, but it is undeniable that it financially benefitted from it by attracting some users. This is sufficient to subject Hotfile to vicarious liability under the first prong of the analysis.

As for the second prong – the right to control user conduct and failure to do so – Hotfile contends that there is a triable issue because Hotfile's content-neutral approach meant that Hotfile could not determine which files were infringing, thereby depriving it of the ability to control the infringement. However, a reading of the common law standard suggests that courts have viewed this element expansively, finding that service providers have the capacity to control the activities of their users simply by virtue of providing the means to commit direct infringement. *See, e.g., Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc.*, 443 F.2d 1159, 1173 (2d Cir. 1971)*; Polygram Int'l Publ'g*

Inc. v. Nevada/TIG, Inc., 855 F. Supp. 1314, 1328 (D. Mass. 1994) (reviewing case law, quoting the legislative history of the Copyright Act, and concluding that a defendant has "control" if they "either actively operate or supervise the operation of the place wherein the performances occur, *or* control the content of the infringing program").[26]

For example, in *Usenet.com*, the defendants maintained online bulletin boards from which users (with a subscription) could download copyrighted sound recordings. 633 F. Supp. 2d at 130-131. As sufficient evidence of the right to control, the court noted that the defendants had a policy that prohibited the sharing of copyrighted content; maintained computer servers that stored and transmitted user-originated content; possessed the ability to filter or block content, including infringing content; and "at times, exercised their right and ability to restrict, suspend, or terminate subscribers," such as by suspending accounts of spammers, limiting the activity of those who used a disproportionate amount of resources, and restricting downloads of pornographic material. *Id.* at 131, 157. And in the swap meet case, albeit a non-Internet context, the site operator could be held vicariously liable because it "patrolled the premises,"

---

26 It is important to note that Section 512(c)(1)(B) of the DMCA excludes from safe harbor those who "receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity." 17 U.S.C. § 512(c)(1)(B). Although phrased in a similar way to the common law vicarious liability standard, courts have read it in the context of other portions of the DMCA to not foreclose protection for service providers that would be vicariously liable for users' infringing activity (without "something more than the ability to remove or block access to materials posted on a service provider's website"). *Viacom*, 676 F.3d at 38 (quotation omitted); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013). This not only demonstrates the breadth of each prong of the common law doctrine, but also indicates that the DMCA precedent Hotfile relies on in its brief is inapplicable to the discussion here. *See Capitol Records, Inc. v. MP3tunes, LLC*, No. 07 Civ. 9931 (WHP), 2013 WL 1987225, at *10 (S.D.N.Y. May 14, 2013).

"controlled the access of customers to the swap meet area," and "had the right to terminate vendors for any reason whatsoever and through that had the ability to control the activities of vendors on the premises." *Fonovisa*, 76 F.3d at 262.

Beyond the right to exclude, the ability to control must be real and practical. In *Perfect 10 v. Amazon.com, Inc.*, for instance, Google allowed users to search for images (including infringing images) on others' websites, but could not prevent those websites from posting infringing content and did not possess image-recognition technology that could precisely block its users' access to those images. 508 F.3d at 1174. The court stated that the alleged offender must have "both a legal right to stop or limit the directly infringing conduct, as well as the practical ability to do so." *Id.* at 1175. Thus, Google was not vicariously liable because it could not control the activities of the direct infringers (although it could have been contributorily liable to the extent it materially assisted them). *Id.* at 1174-75. And in *Luvdarts, LLC*, the Ninth Circuit ruled that mobile wireless carriers could not be held vicariously liable for the acts of their subscribers who allegedly shared access to plaintiffs' protected works. 710 F.3d at 1071-72. Even though the infringement occurred over the service networks that the defendants ran, the defendants had no way of supervising user activity or implementing a system to prevent infringement.

The analysis here, based on precedent, is straightforward. Hotfile controls the means of infringement by among other things mandating user registration and hosting the infringing materials on its own servers. *Cf. Amazon.com, Inc.*, 508 F.3d at 1174 (distinguishing *Napster*, 239 F.3d at 1023-24). Moreover, Hotfile has a stated policy that permits it to control user activity (and, as in *Fonovisa*, to exclude users) and

maintains that it has exercised that control in policing content. Hotfile has also adopted technology that it claims is effective in filtering and targeting infringing works. These actions, which benefit Hotfile in an assessment of direct liability, belie Hotfile's argument that it lacks control because it has no search function and no way to identify or remove infringing files. It is also clear that prior to the filing of the Complaint, Hotfile failed to properly exercise its control in light of the number of users who were blatantly infringing and the estimates of the Studios' experts regarding the prevalence of protected content available for download. Accordingly, on this record, the Studios have made a case for vicarious liability, and summary judgment is entered in their favor.

C. Anton Titov's Individual Liability

In addition to the corporate entity, Hotfile Corp., the Studios have sued Titov in his individual capacity, seeking to extend any damages that may be awarded against Hotfile. Titov has filed a separate motion for summary judgment on the issue of his liability. In this Circuit, "a corporate officer who directs, controls, ratifies, participates in, or is the moving force behind the infringing activity, is personally liable for such infringement." *Babbit Elecs., Inc. v. Dynascan Corp.*, 38 F.3d 1161, 1184 (11th Cir. 1994) (citation omitted); *Southern Bell Tel. & Tel. Co. v. Assoc. Tel. Directory Publishers*, 756 F.2d 801, 811 (11th Cir. 1985). While much of this precedent concerns corporations that directly violate others' copyrights, it is equally applicable to entities liable for secondary infringement. *See Usenet.com*, 633 F. Supp. 2d at 158-59 (holding that director and sole shareholder of companies operating online bulletin boards where infringement occurred was liable under theories of direct and secondary liability for copyright infringement). The secondary infringement theory focuses on the effect the

individual had on the decision to commit infringement and looks beyond the corporate form and principles of limited liability. *See Babbit Elecs., Inc.*, 38 F.3d at 1184 (citation omitted).

Alternatively, a person may be liable under a vicarious liability theory if he is responsible for supervising the infringing activity and benefits from it, even if he is "ignorant of the infringement." *Southern Bell*, 756 F.2d at 811 (citations omitted); *see also Gershwin Pub'g Co.*, 443 F.2d at 1162 ("For example, a person who has promoted or induced the infringing acts of the performer has been held jointly and severally liable as a 'vicarious' infringer, even though he has no actual knowledge that copyright monopoly is being impaired.") As courts have recognized,

> A corporate officer may be held vicariously liable under the Copyright Act when: (1) the officer personally participated in the actual infringement; or (2) the officer derived financial benefit from the infringing activities as either a major shareholder in the corporation, or through some other means such as receiving a percentage of the revenues from the activity giving rise to the infringement; or (3) the officer used the corporation as an instrument to carry out a deliberate infringement of copyright; or (4) the officer was the dominant influence in the corporation, and determined the policies which resulted in the infringement; or (5) on the basis of some combination of the above criteria.

Marvin Music Co. v. BHC Ltd. P'ship, 830 F. Supp. 651, 654-55 (D. Mass. 1993) (summarizing case law) (quotation omitted).

Defendants attempt to minimize Titov's role, arguing that he is an "engineer," "technologist," "employee," or "accountant," rather than a key officer, involved only in "routine" administrative matters; that he did not provide the start-up capital or conceive of the idea for Hotfile; that he holds no sway over Hotfile either at the top-level or with respect to its day-to-day operations; and that [redacted] Defendants' argument rests both on an assertion that Titov

did not have personal involvement in the decisions giving rise to liability and that the group dynamic and the presence of more culpable figures [redacted] mean that Titov could not have had the requisite degree of control over the company's decisions to warrant liability.

Defendants illustrate their argument by citing *Mozingo v. Correct Manufacturing Corporation*, 752 F.2d 168 (5th Cir. 1985), which involved a products liability claim against a work platform manufacturer and its president. There, the plaintiff established that the product was defective at trial, but the district court directed a verdict on the issue of the president's personal liability, applying a Mississippi doctrine that requires that an officer "directly participates in or authorizes the commission of a tort." *Id.* at 171-73. The evidence showed that the president organized and owned predecessor companies that manufactured the defective product. *Id.* at 172-73. Moreover, the president expressed "some reservations concerning the unit's safety" during its development – possibly touching on the nature of the defect – and "authorized the production of a single prototype unit." *Id.* at 173. Nevertheless, the district court characterized his involvement in the development and manufacturing processes as "peripheral" and cited his lack of awareness that the product was put into production. *Id.* at 174. In affirming, the Fifth Circuit reasoned that "[i]f [the president] can be held personally liable in this case, any corporate officer who fails to maintain an almost total ignorance of the products the corporation produces may be personally liable in the event a defective product is produced." *Id.*

---

[27] The Studios explain that they have not brought suit against these shareholders because Hotfile proffered Titov as its public face and the Studios only recently discovered these shareholders' identities.

However, authority involving copyright infringement is not as stringent in holding relevant corporate principals liable. For example, in *Quartet Music v. Kissimmee Broadcasting, Inc.*, 795 F. Supp. 1100 (M.D. Fla. 1992), a group of music publishers brought suit against a radio station and its president for broadcasting music in a manner inconsistent with a licensing agreement. *Id.* at 1101. Issuing a decision after a bench trial, the court juxtaposed the Eleventh Circuit's decision in *Southern Bell* and two district court cases, *Warner Brothers Inc. v. Lobster Pot Inc.*, 582 F. Supp. 478 (N.D. Ohio 1984), which imposed liability against a president who oversaw a restaurant where unauthorized performances of music were held, and *Broadcast Music, Inc. v. Behulak*, 651 F. Supp. 57, 61 (M.D. Fla. 1986), which, by contrast, immunized a corporate officer who was merely a "silent partner" in the lounge where infringement occurred. *Quartet Music*, 795 F. Supp. at 1103-04. The court concluded that the president was liable for copyright infringement notwithstanding his corporate role because of his participation in the activities of the business and the conduct at issue; he had been involved in litigation concerning similar claims, his company had been given notice of the alleged infringement, he ran the radio station's operations, and he had the right to supervise the infringing activity. *Id.* at 1104.

While *Quartet Music* involved a single owner with exclusive control over the infringing activities, one judge in this district has observed that "*Southern Bell* does not require ultimate authority, nor does it require only one person to have authority." *Foreign Imported Prods. & Publ'g, Inc. v. Grupo Indus. Hotelero, S.A.*, No. 07-22066 CIV, 2008 WL 4724495, at *14 (S.D. Fla. Oct. 24, 2008). Numerous other courts support that proposition. *See, e.g., Columbia Pictures Indus., Inc. v. Redd Horne, Inc.*,

749 F.2d 154, 160 (3d Cir. 1984) (affirming order imposing liability against both the president and sole shareholder of a defendant entity, as well as his brother, who was not a stockholder or officer but gave the impression that he was a principal in the business venture); *Pickwick Music Corp. v. Record Prods., Inc.*, 292 F. Supp. 39, 41 (S.D.N.Y. 1968) (finding liability for three defendants who formed and ran a corporation, although they had different responsibilities for recording, editing, and selling an infringing record, but not two others who had "performed merely ministerial office functions"). "Corporate officers have been held liable for the copyright infringement committed by their corporate entity in a variety of situations." *Blendingwell Music, Inc. v. Moor-Law, Inc.*, 612 F. Supp. 474, 482 (D. Del. 1985) (parenthetically citing examples). By contrast, Defendants point to no precedent suggesting that a multitude of culpable actors – and thus, the lack of a single "central figure" – is determinative of liability.

Moreover, Defendants' contention that the particular facts of this case make it incomparable to any other is unpersuasive, since the hallmarks of participation, control, and benefit are undeniably present here. First, Titov is a high-ranking, central figure at Hotfile. He owns a stake in the company nearly as large as its other [redacted] shareholders and runs it in equal part; [redacted] and govern Hotfile by consensus. In his role, Titov has advanced, rejected, agreed upon or failed to block every decision that has shaped the company, including the efforts Hotfile took to identify and remove infringing content, implementing and eventually eliminating the master file policy, and deciding how to reward Hotfile's affiliates. Moreover, Titov [redacted] was indispensable in the company's formation, crucial to the development of its business model, and continues to be involved in its business

strategy. Titov acknowledges possessing power of attorney for the company and acting as its manager when authorized.

In addition, Titov has personally had a hand in every aspect of the conduct underpinning the Studios' theories of liability in this case. For example, at the outset, Titov wrote the programming code that runs the Hotfile interface and enables direct infringers to upload and download protected works. More recently, he undertook a management role in which he oversees contractors working for Hotfile and participates in maintaining Hotfile's storage and delivery technology. Titov also has a significant impact in his work for Hotfile's related entities. He is the sole owner, manager and director of Lemuria, which owns and maintains the servers on which the infringing files at issue are stored, and he is the managing director of Hotfile Ltd., which collects subscription fees from users and pays affiliates. Together, these companies provide mechanisms necessary for Hotfile to collect its revenue, for its users to access its services, and for the entire system to sustain business and grow.

The Studios have also pointed to specific evidence showing Titov's actual awareness of infringement on Hotfile's network. For example, he understood from his conversations with [redacted] that Hotfile acquired users migrating from Rapidshare when that network was sued for infringement. He also expressed the concern that Hotfile would become the "flagship" for non-licensed content and was a party to communications claiming that certain files were infringing. Significantly, Titov appears on nearly every document that the Court considered in determining liability. Titov also put in place Hotfile's DMCA agent, who received millions of infringement notices. Thus, while the Court acknowledges that Titov may not have gone so far as to personally

engage in acts of direct infringement, and that any one of his functions might not give rise to liability on its own, the totality of the circumstances supports liability. In contrast to other cases, his role is not peripheral, his function is not that of merely a silent shareholder or ordinary employee, and his duties are not just ministerial.

The Studios have shown sufficient financial benefit and control for the Court to conclude that Titov is liable under a vicarious liability theory. With regard to the first requirement – financial benefit – the evidence shows that as the company earned money from new subscriptions (some portion of which was attributable to the availability of infringing materials), so did Titov. Titov also instructed employees to ban one user, demonstrating his ability to block or exclude Hotfile's clientele. And, as noted previously, the record shows Titov's impact in determining Hotfile's policies and his dominant influence on the corporation. To the extent that Hotfile can be found liable on any of the theories discussed above, the Court finds that Titov was a critical actor in the underlying operations. Thus, there are no disputed facts that preclude a finding that Titov is vicariously liable for the acts of infringement occurring on Hotfile's network.

In a final effort to avoid liability, Defendants contend that Titov – a Russian citizen who resides in Bulgaria – is not subject to personal jurisdiction in Florida. Titov has advanced this assertion at least twice in this case: as a defense in his Answer and by asking the Studios not to serve him while he attended mediation in this jurisdiction. However, Titov failed to address the issue in the motion to dismiss he filed on March 31, 2011 (DE 50), which challenged only whether the Complaint stated a claim for relief under Federal Rule of Civil Procedure 12(b)(6). Federal Rule of Civil Procedure 12(h) provides that a party waives certain defenses that could have been raised under Rule

12(b) – such as lack of personal jurisdiction – by failing to interpose them in the first pleading. Rule 12(h) is explicit, requires compliance, and means that Titov has procedurally waived the personal jurisdiction issue. *See, e.g., Boston Telecomms. Grp., Inc. v. Deloitte Touche Tohmatsu*, 249 F. App'x 534, 537 (9th Cir. 2007) (reversing district court's finding of non-waiver of personal jurisdiction where counsel had not seen a copy of the complaint, moved to dismiss for insufficiency of process, and stated that he reserved the right to file a supplemental motion to dismiss).

Moreover, a long litany of cases establishes the common law principle that a party waives such a defense by appearing generally and litigating the merits of a claim, as Titov has done here. *See, e.g., Ins. Corp. of Ireland, Ltd. v. Compagnie des Bauxites de Guinee*, 456 U.S. 694, 706 (1982) (noting that where personal jurisdiction is lacking, the defendant has the choice of ignoring the proceedings and raising a collateral challenge in enforcement proceedings or appearing specifically to challenge personal jurisdiction).[28] After stumbling upon a personal jurisdiction challenge buried deep in the summary judgment briefing, the Court finds no indication that Titov is

---

[28] In *Gerber v. Riordan*, 649 F.3d 514 (6th Cir. 2011), for example, a *pro se* defendant filed a motion to dismiss for lack of personal jurisdiction, which was denied for procedural reasons. The defendant then obtained an attorney who entered an appearance, moved to stay pending arbitration, sought to vacate a default judgment that had been entered, opposed a request for mediation, participated in a case management and pretrial conference, sought to enforce a settlement agreement, and engaged in discovery. *Id.* at 518-19. After noting the lack of precedent in the area, the court considered whether filings and appearances that are distinct from jurisdictional challenges – such as anything that would "cause the court to go to some effort that would be wasted if personal jurisdiction is later found lacking" – waive a personal jurisdiction defense. *Id.* at 519 (citations and quotation omitted). While some of those actions might have indicated that the party did not submit to the court's jurisdiction or that the defendant sought merely to postpone the case, the filing of a general appearance "constituted a voluntary acceptance of the district court's jurisdiction."

avoiding a defense of the suit on the merits. To the contrary, in asserting defenses, filing motions related to the record, and personally attending oral argument, Titov has submitted to – has invoked – the jurisdiction of this Court. The Court finds Titov's contentions that this was the "first available opportunity" to raise the issue and that the Studios "have waived any waiver argument" disingenuous. If any issue could be deemed waived, this is and he has.

D. Hotfile's Counterclaim

And finally, the Court turns to Hotfile's counterclaim against Plaintiff Warner. Notices of infringement are a prominent feature of the DMCA. The statute spells out six elements for a notice to be effective, specifies requirements the service provider must meet so that it may properly receive notice, requires service providers to act on receipt of notices such as by removing infringing users' content, and provides a procedure for challenging copyright owners' designations. Providing the legal basis for Hotfile's counterclaim, Section 512(f) sets out a private cause of action for anyone who is injured by a material representation that content or activity is infringing when it is not:

> Any person who knowingly materially misrepresents under this section . . . that material or activity is infringing . . . shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.

17 U.S.C. § 512(f).

Section 512(c), dealing with the creation of notices, requires that notices be accompanied by "[a] statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright

owner, its agent, or the law." 17 U.S.C. § 512(c)(3)(A)(v). Nonetheless, Section 512(f) does not impose liability for issuing a defective notice *per se*, only for making false claims of infringement. According to the statute's legislative history, the subsection "establishes a right of action against any person who knowingly misrepresents that material or activity is infringing" and "is intended to deter knowingly false allegations to service providers in recognition that such misrepresentations are detrimental to rights holders, service, providers, and Internet users." S. Rep. No. 105-190 (1998) at 50. In this regard, Hotfile claims that Warner had actual knowledge that the identified notices were false and asserts that it was damaged as a result. Warner, conversely, has moved for summary judgment on the ground that Hotfile cannot make a sufficient showing to establish its claim.

Preliminarily, the parties, like the Court, have grappled with several issues surrounding enforcement of Section 512(f), which is not well understood. *See Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678, 704 (D. Md. 2011) ("There is not a great deal of case law interpreting [Section 512(f)]."); *UMG Recordings, Inc. v. Augusto*, 558 F. Supp. 2d 1055, 1065 (C.D. Cal. 2008), *aff'd on other grounds*, 628 F.3d 1175 (9th Cir. 2011) (noting "uncertainty" in the area of law). For instance, both sides recognize that the statute requires actual, subjective knowledge of the fact of noninfringement at the time that a takedown notice is made, based upon the theory that one cannot knowingly misrepresent what one does not understand to be false. *See Rossi v. Motion Picture Ass'n of Am., Inc.*, 391 F.3d 1000, 1004-05 (9th Cir. 2004) (holding that the statute "encompasses a subjective, rather than objective

[reasonableness] standard").[29] Indeed, mistakes, even "unreasonable" mistakes, do not necessarily call for liability, so long as they are honestly believed. *Id.* (citing 17 U.S.C. § 512(f)).

But Hotfile asks whether certain "egregious" attributes of Warner's system that might have prevented it from *acquiring* subjective knowledge (such as not relying on human review, failing to download mistaken files, and failing to examine file titles) unjustly insulate Warner from liability for unreasonable mistakes. *Compare, e.g., Online Policy Grp. v. Diebold, Inc.*, 337 F. Supp. 2d 1195, 1204 (N.D. Cal. 2004) ("'Knowingly' means that a party actually knew, should have known if it acted with reasonable care or diligence, or would have had no substantial doubt had it been acting in good faith, that it was making misrepresentations."), *with Cabell*, 2010 WL 996007, at *4 ("[N]egligence is not the standard for liability under section 512(f)." (citation omitted)), *and Augusto*, 558 F. Supp. 2d at 1065 (holding that allegations that the counterclaim-defendant "should have known better do not create a genuine issue of material fact"). Hotfile also asks

---

[29] In *Rossi*, which is the case cited most often in this area, the owner of a website directory sued a movie studio trade association that followed the DMCA's notice and takedown procedures, contending that any reasonable investigation of his website would have revealed that it did not link to infringing content. *Id.* at 1003. Considering Section 512(f)'s express language and interpretive case law dealing with a wide variety of similarly-worded statutes, the Ninth Circuit held that the statute employs an objective standard and ruled against the plaintiff. *Id.* at 1004-05 (stating that the statute protects "potential violators from subjectively improper actions by copyright owners"). Instead of subjective knowledge of noninfringement, one of the association's members notified it of possible infringements on the subject website and the website itself suggested to users that protected movies could be downloaded by joining. *Id.* The clear lesson of *Rossi* is that "as a prerequisite to liability under section 512(f), a defendant must have actual knowledge that it is making a misrepresentation of fact." *Cabell v. Zimmerman*, No. 09 Civ. 10134 (CM), 2010 WL 996007, at *4 (S.D.N.Y. Mar. 12, 2010) (citations omitted).

whether Warner's actual knowledge of its rate of false positives – attributable to search terms it knew were, at times, overbroad as well as its practice of deleting surrounding files – can raise an inference that Warner is liable for possessing guilty knowledge or support liability under a willful blindness theory.

Some courts have cited Section 512(c) to suggest liability where a party did not develop a "good faith" or "sufficient" basis to believe infringement before submitting a notice. *See Dudnikov v. MGA Entm't, Inc.*, 410 F. Supp. 2d 1010, 1013 (D. Colo. 2005) (holding, in the context of a Section 512(f) claim, that the defendant "was required to show that it had a sufficient basis to form the required good faith belief that the plaintiffs' auction infringed on its rights, and that its actions therefore complied with the notice and takedown requirements under the DMCA); *but see Augusto*, 558 F. Supp. 2d at 1065 ("Congress included an expressly limited cause of action for improper infringement notifications, imposing liability only if a copyright owner's notification is a knowing misrepresentation." (quotation and citations omitted)).[30] One court, in a series of four decisions, went so far as to hold that prior to submitting a takedown notice, the copyright holder must consider not only whether the material actually belongs to it, but whether the use of the material lacks an obviously lawful purpose like fair use. *See Lenz v. Universal Music Corp.*, 572 F. Supp. 2d 1150 (N.D. Cal. 2008) ("*Lenz I*") (denying motion to dismiss); *Lenz v. Universal Music Corp.*, No. C07-3783 JF(RS), 2008 WL 4790669 (N.D. Cal. Oct. 28, 2008) ("*Lenz II*") (denying motion for interlocutory appeal); *Lenz v. Universal Music Corp.*, No. C07-3783 JF, 2010 WL 702466 (N.D. Cal.

---

30 *Rossi* itself noted the fact that the defendant in that case had not actually downloaded the files, but went on to describe other compelling facts that led the defendant to believe that infringement of its works was occurring.

Feb. 25, 2010) ("*Lenz III*") (granting plaintiff's motion for partial summary judgment on affirmative defenses); *Lenz v. Universal Music Corp.*, No. 5:07-cv-03783-JF, 2013 WL 271673 (N.D. Cal. Jan. 24, 2013) ("*Lenz IV*") (denying motions for summary judgment).[31]

Thus, if Warner had some similar type of duty, it might find itself vulnerable to suit because its pre-notice review was minimal and swift, consisting of mechanically reviewing the titles and superficial attributes of files. Moreover, even if its methodology were reliable, Warner was concerned with determining whether it *owned* the works rather than whether the use of the works *infringed* on its copyrights to support a proper 512(c) claim. *See Sony/Betamax*, 464 U.S. at 433 ("[A]nyone . . . who makes a fair use of the work is not an infringer of the copyright with respect to such use."); *Amaretto*

---

[31] In that case, Stephanie Lenz, a user of the Internet video hosting site YouTube, uploaded a video of her family dancing to a song performed by the music artist Prince, which turned out to be wildly popular among viewers. *Lenz I*, 572 F. Supp. 2d at 1152. The owner of the song, Universal Music Corporation, sent a takedown notice to the service provider, which notified Ms. Lenz that her video had been removed because of a claim of copyright infringement. *Id.* Discovery revealed that Universal had an employee who was tasked with using YouTube's system to search for titles owned or administered by Universal. *Lenz IV*, 2013 WL 271673, at *1. He stated that he issued a takedown notice whenever he could recognize a one second or longer portion of a Prince song in any video, as occurred in the video at issue. *Id.* at *5. His boss stated that Universal seeks to remove songs "when a writer is upset or requests that particular videos be removed from YouTube," prompting Universal to conduct a review. *Id.*

The court concluded that summary judgment in favor of either party was improper. Ms. Lenz could show that Universal's procedures might have willfully blinded it to knowledge of her fair use, but not that Universal subjectively believed that there was a high probability that the video was lawful or that the nature of fair use was self-evident. *Id.* at *6-7 (citing *Viacom*, 676 F.3d at 34). Likewise, Universal could not demonstrate the absence of subjective intent. *Id.* at *8.

Ranch Breedables, LLC v. Ozimals, Inc., 790 F. Supp. 2d 1024, 1029 (N.D. Cal. 2011) (noting that a Section 512(f) plaintiff can contest the validity of a takedown notification even where a valid copyright exists). And, Warner's reliance on technology to accomplish the task might prevent it from forming any belief at all, as the *amicus curiae* argues here and a similar group asserted in *Rossi*: "computers conducting automated searches cannot form a belief consistent with the language of the DMCA, because they cannot distinguish between infringing content and content that merely contains words that suggest infringement." *Rossi*, 391 F.3d at 1005 n.7. The Court, however, is unaware of any decision to date that actually addressed the need for human review, and the statute does not specify how belief of infringement may be formed or what knowledge may be chargeable to the notifying entity.

Ultimately, while these are engaging questions surrounding Warner's knowledge; its responsibility to investigate; whether it had a good faith belief in infringement in each instance; and whose burden it is to show or refute what – all issues of first impression in this Circuit – there is sufficient evidence in the record to suggest that Warner intentionally targeted files it knew it had no right to remove. This precludes summary judgment in its favor. Specifically, Hotfile has provided the example of JDownloader, which Warner did not manage and acknowledged removing for reasons unrelated to copyright infringement. It has also shown Warner's interest in an application of its takedown rights beyond works that it owns. And Warner has not otherwise argued that it had the right to remove those files, only that its mistakes should be excused. The Court finds this motive and other evidence sufficient to sustain an inference that Warner violated Section 512(f), such that these issues should be presented to the jury.

The only issue remaining is whether Hotfile is able to show any injury for the deletions, which is an element of a Section 512(f) claim and which Warner questions. "A fair reading of the statute, the legislative history, and similar statutory language indicates that § 512(f) plaintiff's damages must be proximately caused by the *misrepresentation to the service provider and the service provider's reliance on the misrepresentation.*" *Lenz III*, 2010 WL 702466, at *10 (emphasis in original). In this regard, the Court observes that the quantity of economic damages to Hotfile's system is necessarily difficult to measure with precision and has led to much disagreement between the parties and their experts. Notwithstanding this difficulty, the fact of injury has been shown, and Hotfile's expert can provide the jury with a non-speculative basis to assess damages. Additionally, *Lenz III* concluded that the subsection provides for damages beyond actual damages, even if they are not substantial. *Id.* at *7-10. On this basis, the Court concludes that Warner is unable to establish the absence of a genuine dispute on the issue of damages and cannot prevail at this juncture.

III. CONCLUSION

In accordance with the foregoing, it is hereby **ORDERED AND ADJUDGED** as follows:

(1) Hotfile's motion for partial summary judgment for post-Complaint DMCA protection (DE 275, DE 318), Defendant Anton Titov's motion for summary judgment on personal liability (DE 276, DE 316), and Warner's motion for summary judgment as to Hotfile's counterclaim (DE 255, DE 301) are **DENIED**.

(2) Plaintiffs' motion for summary judgment (DE 280, DE 322) is **GRANTED** as to the issues of Defendants' DMCA defense, vicarious liability, and Mr. Titov's liability. It is **DENIED** in all other respects.

(3) Except to the extent addressed herein, Defendants' motions to strike Dr. Waterman's rebuttal report (DE 217); to strike Dr. Foster's reply declaration (DE 452, DE 460) and certain exhibits (DE 339) in connection with Plaintiffs' summary judgment briefing; and to strike certain exhibits in connection with Plaintiffs' opposition to Mr. Titov's summary judgment motion (DE 371), are **DENIED AS MOOT**. Similarly, Plaintiffs' motion to strike portions of the declarations of Dr. Andrew Cromarty, Dr. Boyle, and Mr. Titov (DE 387, DE 423) is **DENIED AS MOOT**.

(4) Warner's motion to use an exhibit from Mr. Titov's deposition at trial (DE 241, DE 297) is **GRANTED**, and Plaintiffs' Objections to Judge Turnoff's Report and Recommendation (DE 327, DE 370) are **OVERRULED**. Judge Turnoff's Report and Recommendation (DE 306) is **ADOPTED AND AFFIRMED**.

(5) The parties shall confer and provide to the Court proposed redactions to this Order within **fourteen (14) days** of the date of this Order, so that the Court can issue a public version of this decision.

DONE AND ORDERED in chambers in Miami, Florida, this 20th day of August, 2013.

KATHLEEN M. WILLIAMS
UNITED STATES DISTRICT JUDGE

EXHIBIT F