EXHIBIT I

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

LIBERTY MEDIA HOLDINGS, L.L.C.	*	
A California Limited Liability Co.,	*	
	*	
Plaintiff,	*	
	*	
VERSUS	*	
	*	
HOTFILE.COM,	*	
A Foreign (Panama) Corporation,	*	TRIAL COURT CAUSE:
ANTON TITOV,	*	
A Foreign Individual,	*	3:09-CV-2396-D
WEBAZILLA, L.L.C.,	*	
A Florida Limited Liability Company,	*	
WEBAZILLA, B.V.,	*	
A Foreign (Dutch) Corporation,	*	
MONIKER ONLINE SERVICES,	*	
A Florida Limited Liability Company,	*	
LIMELIGHT NETWORKS,	*	
An Arizona Corporation,	*	
PAYPAL, INC.,	*	
A California Corporation,	*	
DRAGOS BADAN,	*	
An individual,	*	
VINICIUS ALVES,	*	
An individual,	*	
JOSEF DAVIS S. PRADE,	*	
An individual ,	*	
ROBERT PARELL,	*	
An individual ,	*	
YUNZHI COMPUTER,	*	
An individual ,	*	
SHALLALAT GEN TR, L.L.C,,	*	
An individual,	*	
ASHISH THAKUR,	*	
An individual ,	*	
SATHEESH D N,	*	
An individual,	*	
KEYANA IT CO. LTD.,	*	
An individual,	*	
PREMIUM ISSUER ,	*	
An individual ,	*	

MUHAMA KHAIRUL IBRAHIM,	*
An individual,	*
TOUCH DIAMOND LIMITED,	*
HOTFILE PREMIUM,	*
AYDINLAR KIRTASIYE OFFICE,	*
OZGUR,	*
TAMER ÇEKICI,	*
FATIH OKTEN,	*
JOHN DOE, numbers 1-500,	*
Presently unknown Defendants.	*
	*
Defendants.	*
	*

NOTICE OF FILING PLAINTIFF'S CORRECTED REPLY BRIEF TO OPPOSITION TO MOTION FOR PRELIMINARY INJUNCTION

LEAD COUNSEL:
Marc J. Randazza, Esq.
302 Washington Street, Suite 321
San Diego, CA 92103
Telephone:619-866-5975
Facsimile: 619-866-5976
Electronic Mail: marc@corbinfisher.com
Massachusetts Bar Card No.: 651477
Florida Bar Card No.: 625566
Admitted to practice before the
United States District Court
Northern District of Texas

LOCAL COUNSEL:
Gary P. Krupkin, Esq.
1116 Commerce Drive
Richardson, Texas 75081
Telephone: 972-261-8284
Facsimile: 972-671-3671
ElectronicMail:krupkinlaw@gmail.com
Texas Bar Card No.: 00790010
Admitted to practice before the
United States District Court
Northern District of Texas

Notice of Filing Corrected Reply Brief

The Plaintiff erroneously filed its Reply Brief with a number of errors. The errors occurred due to the fact that the Brief was filed late at night, and in the compressed briefing schedule, the rush caused a number of errors to be made - most notably, the original Reply Brief was filed with some URLs listed that contained vulgarity. Per the Court's Order and the Plaintiff's Letter Brief on this issue, documents containing vulgarity will be either redacted or filed under seal. Unfortunately, URLs can not be redacted, lest they no longer function.

The Corrected Reply Brief resolves this issue, and a few other important errors in the original Reply. The errors were inadvertent, and upon detection, the Undersigned and his staff immediately filed the Corrected Reply, which should replace and supersede the original. Appendix A is being filed under seal, as it contains vulgarity.

Respectfully submitted,

s/ Marc Randazza

LEAD COUNSEL:
Marc J. Randazza, Esq.
302 Washington Street, Suite 321
San Diego, CA 92103
Telephone:619-866-5975
Facsimile: 619-866-5976
Electronic Mail: marc@corbinfisher.com
Massachusetts Bar Card No.: 651477
Florida Bar Card No.: 625566
Admitted to practice before the
United States District Court
Northern District of Texas

s/Gary Krupkin

LOCAL COUNSEL:
Gary P. Krupkin, Esq.
1116 Commerce Drive
Richardson, Texas 75081
Telephone: 972-261-8284
Facsimile: 972-671-3671
ElectronicMail:krupkinlaw@gmail.com
Texas Bar Card No.: 00790010
Admitted to practice before the
United States District Court
Northern District of Texas

CERTIFICATE OF SERVICE

This is to certify that on the 8th day of February 2010, a true and correct copy of the foregoing document has been served via CM/ECF notification, as well as email service.

s/ Marc Randazza

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

LIBERTY MEDIA HOLDINGS, L.L.C.	*	
A California Limited Liability Co.,	*	
	*	
Plaintiff,	*	
	*	
VERSUS	*	
	*	
HOTFILE.COM,	*	
A Foreign (Panama) Corporation,	*	TRIAL COURT CAUSE:
ANTON TITOV,	*	
A Foreign Individual,	*	3:09-CV-2396-D
WEBAZILLA, L.L.C.,	*	
A Florida Limited Liability Company,	*	
WEBAZILLA, B.V.,	*	
A Foreign (Dutch) Corporation,	*	
MONIKER ONLINE SERVICES,	*	
A Florida Limited Liability Company,	*	
LIMELIGHT NETWORKS,	*	
An Arizona Corporation,	*	
PAYPAL, INC.,	*	
A California Corporation,	*	
DRAGOS BADAN,	*	
An individual,	*	
VINICIUS ALVES,	*	
An individual,	*	
JOSEF DAVIS S. PRADE,	*	
An individual ,	*	
ROBERT PARELL,	*	
An individual ,	*	
YUNZHI COMPUTER,	*	
An individual ,	*	
SHALLALAT GEN TR, L.L.C,,	*	
An individual,	*	
ASHISH THAKUR,	*	
An individual ,	*	
SATHEESH D N,	*	
An individual,	*	
KEYANA IT CO. LTD.,	*	
An individual,	*	
PREMIUM ISSUER ,	*	
An individual ,	*	

MUHAMA KHAIRUL IBRAHIM,	*
An individual,	*
TOUCH DIAMOND LIMITED,	*
HOTFILE PREMIUM,	*
AYDINLAR KIRTASIYE OFFICE,	*
OZGUR,	*
TAMER ÇEKICI,	*
FATIH OKTEN,	*
JOHN DOE, numbers 1-500,	*
Presently unknown Defendants.	*
	*
Defendants.	*
	*

PLAINTIFF'S CORRECTED REPLY BRIEF TO OPPOSITION TO MOTION FOR PRELIMINARY INJUNCTION

LEAD COUNSEL:
Marc J. Randazza, Esq.
302 Washington Street, Suite 321
San Diego, CA 92103
Telephone:619-866-5975
Facsimile: 619-866-5976
Electronic Mail: marc@corbinfisher.com
Massachusetts Bar Card No.: 651477
Florida Bar Card No.: 625566
Admitted to practice before the
United States District Court
Northern District of Texas

LOCAL COUNSEL:
Gary P. Krupkin, Esq.
1116 Commerce Drive
Richardson, Texas 75081
Telephone: 972-261-8284
Facsimile: 972-671-3671
ElectronicMail:krupkinlaw@gmail.com
Texas Bar Card No.: 00790010
Admitted to practice before the
United States District Court
Northern District of Texas

TABLE OF CONTENTS

CORRECTED REPLY BRIEF TO OPPOSITION TO
MOTION FOR PRELIMINARY INJUNCTION

TO THE HONORABLE SIDNEY FITZWATER, JUDGE PRESIDING:

Plaintiff LIBERTY MEDIA HOLDINGS, L.L.C. (hereinafter, "Liberty") by counsel filed this, its REPLY BRIEF TO OPPOSITION TO MOTION FOR PRELIMINARY INJUNCTION as follows:

I. Introduction

The theme of the Defendants' Opposition to Plaintiff's Motion for Preliminary Injunction seems to be four-fold: 1) the court should harbor prejudice against the Plaintiff because of the content of the Plaintiff's films and the sexual orientation approved of therein; 2) the Defendants claim to stop infringing on specific works of the copyright owner finds them first; 3) the Plaintiff is somehow at fault for the Defendant's unlawful activity; and 4) the Defendant can't operate lawfully.

A. The Plaintiff is a Gay Porn producer. So what?

The Defendants' lose no opportunity to remind the court of the Plaintiff's status as an adult entertainment company, which caters to the gay market. See Doc. 42 page 1; Page 2, Page 9 (four times), Page 25, Page 26 (twice). The Defendants' clearly wish to persuade this court that the Plaintiff's property is entitled to less protection than mainstream films, because of its theme. More than 30 years ago, a copyright defendant in this very jurisdiction claimed that the plaintiff's works were legally obscene, and thus not subject to the same copyright protection as non-obscene works. The Fifth Circuit roundly rejected that defense theory. *Mitchell Bros. Film Group v. Cinema Adult Theater*, 604 F.2d 852 (5th Cir. 1979), cert. denied, 445 U.S. 917 (1980).

> It appears to us that Congress has concluded that the constitutional purpose of its copyright power, "(t)o promote the Progress of Science and useful Arts," U.S. CONST. ART. 1, § 8, cl. 8, is best served by allowing all creative works (in a copyrightable format) to be accorded copyright protection regardless of subject matter or content, trusting to the public taste to reward creators of useful works and to deny creators of useless works any reward. *Id*. at 855.

This view was embraced by the Ninth Circuit in *Jartech, Inc. v. Clancy*, 666 F.2d 403 (9th Cir. 1982), cert. denied, 459 U.S. 826 (1982). "The leading treatise on copyright

has called the Fifth Circuit's Mitchell Brothers case 'the most thoughtful and comprehensive analysis of the issue.') (citing Nimmer on Copyright, § 2.17, p. 2-194.2 (1980)).

Given that the content of the Plaintiff's works is irrelevant to the copyright analysis, one must wonder what point the Defendant's are trying to make. It appears clear that the Defendants' are under the belief that if they repeat the words "gay" and "pornography" enough times, that perhaps this honorable Court will find itself psychologically predisposed to find in their favor. As offensive as this notion may be, perhaps it is the Defendants' best card to play, as their other arguments are just as unsound, while lacking the emotional appeal of the school-yard cat-call.

As much as the Defendants wish to sully the image of the Plaintiff, the Defendants should heed the conventional wisdom offered to those who live in glass houses. The Plaintiff profits from the lawful creation and distribution of gay pornography. The Defendants, on the other hand, profit from the illegal copying and illegal distribution of gay pornography.[1] The parties are in the same business, and the only difference is that the Plaintiffs make their profits legitimately and legally – the Defendants can make no such claim.

II. Service of the Complaint and TRO Has Been Effectuated

Though Hotfile and Titov may object to this Court's jurisdiction over him, service has been achieved on both Defendants. If the Court deems that it has not, then the Court should not allow the injunctive relief to expire merely because the Defendants have evaded service.

The Court ordered that the Order be served upon the Defendants pursuant to Rule 5, and that the Complaint be served pursuant to Rule 4. See Doc. 18. Although the Court did not specify that the Complaint could be served under Rule 4(e)(3), this sub-rule is encompassed under the general rule, and given that it is a legal impossibility for service to be achieved in less than six months under traditional international protocols, it was

[1] In addition the Plaintiff responsibly requires that those who view its content provide credit card information and verify that they are over the age of 18 – thus denying minors access to their works. The Defendants, consistent with their "heads in the sand" philosophy, take no such steps.

presumed that the Court intended to authorize the email service requested in the Amended Application for Temporary Restraining Order (Doc. 10).

The Defendants lament that the Plaintiff has not even attempted service beyond its delivery of the relevant documents via email. Opp. at 41. However, Plaintiff has made every possible legal effort to serve the them, including serving the documents by overnight courier to a portfolio of addresses, attempting service by process server, providing them via email, and requesting that their attorney accept service.[2]

A. The Order was properly served under Rule 5.

Fed. R. Civ. P 5(b)(2)(C) deems service complete once notice has been mailed to the recipient's last known address. When Plaintiffs first mailed notice to Hotfile's last known address in Panama, service was complete. *Nichols v. Several Unknown Deputies of the U.S. Marshals Serv.*, 2009 WL 3735803 at *2 n. 3 (W.D. Tex. Nov. 4, 2009) ("service by mail occurs on the date the document was mailed."). See also *Cycle Sport LLC v. Dinli Metal Indus. Co., Ltd*., 2008 WL 4791544 at *3 (N.D. Tex. Oct. 30, 2008) ("mailing the pleading to the person's last known address-in which event service is complete upon mailing") (internal quotations omitted).

Plaintiff mailed notice to the Defendant's Panama location. (Doc. 26 Gapp Dec. re: Contempt ¶¶ 3 and Exh. A thereto.) When this mail was returned to Plaintiff as undeliverable, a process server was sent to search for Defendant. What the process server discovered was that the Panama location did not exist. (Doc. 26 Gapp Dec. re: Contempt ¶ 4 and Exh.s B and C thereto.) See Doc. 43, Exh. 1-A, app. 15. Through mail and in person, Plaintiff twice attempted to serve Defendant at its known physical address. Under Rule 5(b)(2)(C), this should be sufficient. Plaintiff went well beyond what the Rule 5 requires. Courts are particularly amendable to alternate service in the face of the defendant's hiding and subterfuge. See *Ali v. Mid-Atlantic Settlement Serv., Inc*., 233 F.R.D. 32, 36 (D.D.C. 2006). The courts and Federal Rules have no qualms about punishing a defendant for hiding or playing other games in avoidance of a lawsuit. See

[2] Their attorney declined to accept service unless the Plaintiffs would agree to eviscerate the TRO's provisions – rendering the relief granted therein meaningless.

Bailes v. United States, 8 F.3d 20 (5th Cir. 1993) (notice of motion for summary judgment was proper when mailed.

Hotfile did not maintain the proper Panamanian corporate formality of providing the name and domicile of a registered agent in Panama. It seems that given Hotfile's illegal activities, it would prefer to play "hide and seek" with potential plaintiffs -- and that has been its strategy to date. See *Rio Props., Inc. v. Rio Int'l Interlink,* 284 F.3d 1007, 1018 (9th Cir. 2002) ("when faced with an international e-business scofflaw, playing hide-and-seek with the federal court, email may be the only means of effecting service of process.); *Popular Enters. v. Webcom Media Corp., Inc.* 225 F.R.D. 560 (E.D. Tenn. 2004). Hotfile demands formal process to its address in Bulgaria, under the Hague Convention, which can take up to six months. See F*AS Technologies, Ltd v. Dainippon Screen Mfg. Co*., No. 3:98CV2842 2000 WL 193621 (N.D. Tex. Feb. 16, 2000). This tactic is quite clever; the TRO could only last until February 9, but Hague Convention service would take at least half a year.

Furthermore, it is not clear that either Titov or Hotfile are entited to claim that Hague Service applies. Titov's address is unknown. He claims to be a Russian citizen, living in Bulgaria, yet his declaration was signed (apparently) in Amesterdam. (Doc. 43, Exh. 1, App.13.) See Hague Convention Article 1 ("This convention shall not apply where the address of the person to be served with the document is not known.")

Defendant Hotfile is a Panamanian corporation, and as discussed *infra*, Panama is not a member of the Hague Convention. Hotfile claims to do business in Bulgaria, but even the Defendants' pleadings make it clear that the Plaintiffs have not yet discovered Hotfile's address. Defendant states that the Bulgarian address to which the Plaintiff sent the TRO and the Amended Complaint is "Titov and Hotfile's usual address to receive business mail," but does not confess that this is Hotfiles address. Doc. 37 at 7. Therefore Hotfile seems to find no shelter in the Hague Convention protections.

Demanding strict Hague service would mean that the TRO would expire before service was out of its embryonic stage. If the TRO expires, then Hotfile will take its ill-gotten gains and fade into murky obscurity and the harm will continue. See Doc. 15, ¶¶ 2, 4-6. This will, of course, render these proceedings essentially moot. However, US courts have held that service may be effected through alternate means, as long as the

relevant international agreement does not specifically prohibit it. See *Rio Props., Inc.,* 284 F.3d at 1014; *In re Potash Antitrust Litigation*, No. 08 C 6910 2009 WL 358107, 2009 U.S. Dist. LEXIS 102623 (N.D. Ill. Nov. 3, 2009). Furthermore, the corporate defendant, Hotfile, is a Panamanian entity. Panama is not a member of the Hague Convention. It is a signatory to the Inter-American Convention on Letters Rogatory. S. Treaty Doc. 98-27, 98th Cong., 2d sess., (1984), pp. III-V, XII. The Fifth Circuit has held that service by alternate means to Mexico, another Inter-American Convention member, was permitted. "[N]othing in the language of the Convention expressly reflects an intention to supplant all alternative methods of service. Rather, the Convention appears solely to govern the delivery of letters rogatory among the signatory States." *Kreimerman v. Casa Veerkamp, S.A. de C.V.*, 22 F.3d 634, 640 (5th Cir. 1994).

B. The Complaint Was Properly Served Under Rule 4

Under Rule 4(f)(3), the court may order service through means not prohibited by international agreement. Service via e-mail was recognized as a legitimate method of service in *Keller Williams Realty, Incorporated v. Lapeer*, where the court allowed the plaintiff to serve foreign defendants through their last known e-mail addresses. 2008 WL 2944601 at *2 (S.D. Tex. July 31, 2008). This method of service, fulfilling the goal of being "reasonably calculated, under all the circumstances, to apprise interested parties of the pendency of the action and afford them an opportunity to present their objections," satisfied the requirements of Texas Rule 106(b) because it was likely to give defendants actual notice of the suit. *Id*.

Hague Service Convention art. 10(a) excludes postal channels but does not specifically preclude electronic messages. *Id*. Accordingly, e-mail messages should be allowed, as this treaty has not preempted them. See *In re Potash Antitrust Litigation*, No. 08 C 6910 2009 WL 358107 at 15-16, 2009 U.S. Dist. LEXIS 102623 (N.D. Ill. Nov. 3, 2009) (holding that plaintiffs are not required to attempt service through the Hague Convention where a signatory has refused to cooperate for substantive reasons, the court allowed e-mail service upon Russian defendants); see also *In re LDK Solar Sec. Litig*., No. C 07-5182, 2008 WL 2415185 at *2 (N.D. Cal. June 12, 2008) (authorizing alternative means of service on Chinese defendants without attempting service through Hague Convention means, as attempting to do so would be "fruitless").

The *Rio Properties* court specifically stated that electronic service is appropriate when dealing with an "e-business scofflaw, playing hide-and-seek with the federal court." 284 F.3d at 1018. In that case Service by E-mail was appropriate because the defendant did not have a physical location and relied on the computer to operate its business. See also *International Controls Corp. v. Vesco*, 593 F.2d 166, 176-78 (2d Cir. 1979)(approving service by mail to last known address where individual defendant successfully evaded process servers). Other courts have voiced displeasure with jurisdictional games of hide-and-seek, holding that:

> Where service is repeatedly effected in accordance with the applicable rules of civil procedure and in a manner reasonably calculated to notify the defendant of the institution of an action against him, the defendant cannot claim that the court has no authority to act when he has willfully evaded the service of process." *Ali v. Mid-Atlantic Settlement Serv., Inc*., 233F.R.D. 32, 36 (D.D.C. 2006).

These tactics have particularly frustrated courts when plaintiffs, as here, have attempted to serve defendants within the boundaries of applicable law. *Childs v. Cox Communications,* 2006 WL 11030009 at *1 (N.D. Miss. 2006).

The Defendants are properly served. Any concerns about the sufficiency of this method of notice should be put to rest by the Defendant's own actions. The purpose of service under Rule 4(a) is to give a party notice of the proceedings, Defendants' retention of counsel from two separate law firms after receiving electronic service (that they now claim to be inadequate) belies their own argument. The purpose of service – notice of the proceeding – was clearly met. The Due Process Clause only requires that the method of service be reasonably calculated to apprise the interested parties of the action, and afford them an opportunity to voice their objections. See *Mullane v. Central Hanover Bank & Trust Co.*, 339 U.S. 306, 314 (1950). Rule 4 provides for service on foreign defendants by any means that are not prohibited by international agreement. Fed. R. Civ. P. 4(f)(3) and (h)(2). The game is clear: If service has not been effected, and must be effected by retaining Bulgarian government officials for the task (after the documents are translated into Bulgarian at immense cost), the justice sought by the Plaintiff will be impossible to attain - as by then, these criminals will likely have spirited their funds away, never to be seen again.

Finally, as discussed supra, Titov and his conpatriots chose to organize their corporation under the laws of the Republic of Panama. There is no international agreement that prohibits alternate service to Panama, and the Defendants seem to have purposely taken steps to avoid any traditional means of service in Panama. See Doc. 26 Gapp ¶4 and Exh. B and C thereto. Based on these facts, the court should deem Hotfile and Titov served, or now specifically authorize email service to all Defendants.

Defendant has led Plaintiff on a wild goose chase across Panama and Bulgaria, by following up on fake addresses and facts revealed only after Plaintiff has taken action to serve Defendant. This conduct threatens to prejudice Plaintiff's rights in this action. Full compliance with the Hague Convention for service will run beyond the expiration of this Court's TRO. See *Maale v. Francis*, 258 F.R.D. 533, 535-36 (S.D. Fla. 2009) (noting that service and return of proof of service under the Hague Convention normally takes six months or longer, resulting in the court letting the plaintiffs pursue alternate means of service); *Almetals, Inc. v. Wickeder Westfalenstahl*, GMBH 2008 (refusing to dissolve temporary restraining order on defendant's motion because requiring service under the Hague Conventions would require months to complete, while the TRO would end in 20 days).

III. Plaintiff Is Entitled to a Preliminary Injunction

A. Direct Infringement

1. Plaintiff has demonstrated ownership of valid copyrights

Defendants claim that Plaintiff has not identified or demonstrated ownership of any specific works in which it claims copyright protection. See Doc. 42 See III.A.1.a, page 13. Plaintiff's First Amended Complaint (FAC), Exh. M (Doc. 16-6), Infringement Numbers 1151-1272 lists the title of the work owned by Liberty, the URL making the work available on Hotfile.com, and the date Liberty found and downloaded the work from Hotfile.com's system. Moreover, many of the URLs themselves listed in numbers 1-1150 provide the title of the work, the copyright registration number, or both within the URL itself. See Doc. 16-6, Exh. M to the FAC.

Additionally, the DMCA takedown notices (Doc. 43, Exh. 1-J) display the Copyright Certificate number, the title of the work, or both in the subject line of the notice. Additionally, Plaintiff has provided to the Court a representative sampling of

Copyright Registration Certificates. See Doc. 16-2 Exh. D to FAC, and Doc 34-3 Exh. D to Motion for Contempt.[3]

2. The Files Distributed on Hotfile.com are Exact Copies of Plaintiff's Copyrighted Works

As the infringing files made stored on and distributed from Hotfile's system are exact copies if Plaintiff's entire works, this element is easily satisfied. See Doc 34, ¶1.1(a), Doc. 17-1 ¶ 4.8. Additionally, the best evidence of the direct infringement is in the Defendants' own hands, as it resides on the Defendants' servers. This will be produced by the Defendants in discovery unless the Defendants have contemptiuously destroyed evidence. If that is the case, then the Defendants have further violated the TRO, and the factual disputes that this evidence would have supported should be resolved in the Plaintiff's favor. Where evidence is destroyed with evidence of bad faith, an adverse inference is drawn. See *King v. Illinois Cent. R.R.*, 337 F.3d 550, 556 (5th Cir. 2003); *Vick v. Tex. Empl. Com'n*., 514 F.2d 734, 737 (5th Cir. 1975). Additionally, as Plaintiff has found its copyrighted works on Hotfile's system, Plaintiff has downloaded its own works directly from Hotfile to further supplement the evidence and can make copies of these data files available should the Court require further proof on this part.

3. Hotfile is a Direct Infringer

The Uploaders directly infringe by uploading the Plaintiff's works to the Hotfile service. Doc. 34 ¶1.1(a). This creates an illegal copy of the Plaintiff's work. Hotfile provides the uploader with a link. See Opp. at 3-4. The Copyright Act provides that an owner of a copyrighted work has the exclusive right to reproduce the work in copies, to prepare derivative works based on the copyrighted work, to distribute copies of the work to the public, and, in the case of certain types of works, to perform and display the work

[3] The Defendants protestations about some of the titles being partially obscured are without merit. The Plaintiff uses descriptive profanity in its movie titles. This Honorable Court has requested that the Plaintiff take efforts to keep such profanity out of the Court's public records. Doc. 35. The Plaintiff promised this Court that it would. See Plaintiff's February 2, 2010 letter submitted to the Court in response to its request contained it's January 27, 2010 Order (Doc. 31). The Defendants should not point to such efforts as a defensive strategy, especially when the Copyright Registration numbers are clear, and any member of the public could confirm the titles by using the U.S. Copyright Offices publicly accessible copyright database.

publicly. 17 U.S.C. § 106. It also provides that "anyone who violates any of the exclusive rights of the copyright owner as provided by sections 106 through 118 . . . is an infringer of the copyright." 17 U.S.C. § 501(a). *Playboy Enters. v. Webbworld, Inc*., 968 F. Supp. 1171, 1174 (N.D. Tex. 1997). Under the Hotfile scheme, Hotfile reproduces the Plaintiff's works and distributes them to the public. The mere fact that a copyright infringer publishes its illegal copy to only one person does not render it lawful. See *Penguin Books U.S.A. Inc., v. New Christian Church of Full Endeavor*, 288 F.Supp. 2d 544, 556 (S.D.N.Y. 2003) ("A distribution of a work to one person constitutes a publication") citing *Kakizaki v. Riedel*, 811 F.Supp. 129, 131 (S.D.N.Y. 1992); Burke v. Nat'l Broad. Co., Inc., 598 F.2d 688, 691 (1st Cir. 1979). To hold otherwise would mean that all an intellectual property pirate would need to do would be to sub-contract out the mass distribution (as Hotfile does to evade liability completely.

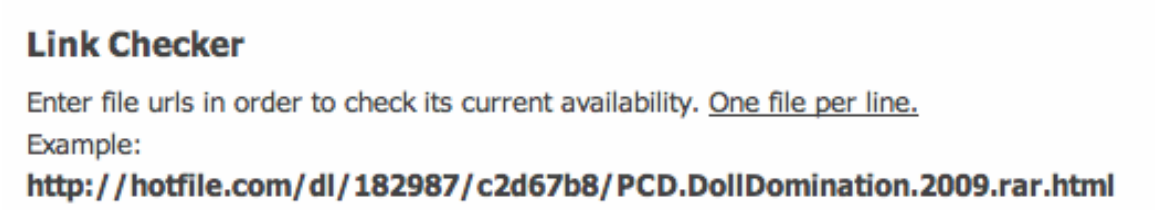
Hotfile attempts to distinguish its activity from the *Playboy Enters. v. Webworld* case by claiming that the Webworld defendant used an automated system to infringe upon Playboy's copyrights, while Hotfile subcontracts the job to other humans. Opp. at 15. However, that very same court (on a motion for partial summary judgment) rejected Hotfile's theory resoundingly and clearly, and in language that needs little modification to fit the case before the court today:

> Webbworld also argues that it cannot be held liable for copyright infringement because it has no control over the persons who are posting the infringing images to the adult newsgroups from which Neptics obtains its material. While this may be true, Neptics surely has control over the images it chooses to sell on the Neptics website. **Even the absence of the ability to exercise such control, however, is no defense to liability**. **If a business cannot be operated within the bounds of the Copyright Act, then perhaps the question of its legitimate existence needs to be addressed.** (emphasis added) 968 F. Supp. at 1175

B. <u>Defendant is willfully blind to the rampant copyright infringement on its site</u>

The Defendant's steps to prevent piracy are woefully inadequate and Hotfile is willfully blind to the copyright infringement that is rampant on its system. Hotfile claims that it could not possibly know about the infringing materials, then claims to know that most of its content is lawful. Opp. at 20. However, it does not take much detective work to simply scratch the surface of the Hotfile enterprise, and find pirated material underneath. The Hotfile website, itself, confirms its predominant use. Hotfile provides a

page where users can check if files have been removed from its system (presumably due to intellectual property claims). See http://hotfile.com/checkfiles.html (last visited February 8, 2010). If one navigates to that page (at least as of the date of this Reply brief) it states:



The example link provided is easily recognized as an album by The Pussycat Dolls – their 2008 release, "Doll Domination."[4] The link to allows anyone to download the entire album for free in 9.7 minutes. If one pays the Hotfile fee, it takes a mere 57 seconds.[5] The Pussycat Dolls sell this very album for $7.99 to $14.99 on their website. http://www.pcdmusic.com/music. The Defendants will not be able to credibly argue that The Pussycat Dolls' record label has given Hotfile permission to distribute it free of charge.

Hotfile compares itself to ocompanies like RapidShare and MegaUpload, both of which are also well-known as illegal file sharing sites – one of which has identical copyright woes. See *Perfect 10 v. Rapidshare AG*, Case No. 09-CV-2596 (S.D. Cal., filed November 18, 2009). In addition to the California case, RapidShare has been dealt a blow by a German court and faces severe penalties if it fails to take appropriate measures against the uploading of copyrighted content by its users. A Hamburg court ruled against RapidShare in a case brought by the German version of the Recording Industry of America, GEMA. See Oberlandesgericht [OLGZ] [Higher Regional Court of Hamburg], July 2, 2008, Az. 5 U 73/07, (F.R.G.).

The Defendants claim that when content is uploaded to Hotfile, "[i]t does not require any identifying information for the uploaded file." See Doc. 42 at 4. Of course Hotfile does not require any identifying information for the uploaded file – nor for the uploading party – and therein lies a portion of Hotfile's complicity, encouragement,

[4] See http://www.pcdmusic.com/music; http://en.wikipedia.org/wiki/Pussycat_Dolls
[5] See http://hotfile.com/dl/182987/c2d67b8/PCD.DollDomination.2009.rar.html

assistance, and willful blindness. See Doc 34, ¶¶ 4.11(B)-4.12(B), Doc. 13, and Exh. F. Hotfile claims that it does not know what files its users upload, and this may very well be true. But, Hotfile cannot claim with any credibility that it would want to know either. Hotfile could ask its users for this information and conduct some form of policing. Hotfile chooses not to because if Hotfile's uploaders believed that they could get caught, they would run for the hills, and if the top 100 most downloaded files were checked, they would certainly be pirated files.

Hotfile claims that it generates revenue by selling faster download speeds. (Doc. 42 at 5.) The Plaintiff agrees – but this is where the agreement breaks down. Hotfile claims that its "revenue does not vary depending either on the type or quality of content that its users upload, store, or download." (Titov Dec. Exh. 1, App. 7, ¶ 28). However it is the pirated content that acts as the bait for the swarm of intellectual property parasites that nest on Hotfile. Similarly, Hotfile claims that "an individual could use Hotfile as a secure file backup site…" Doc. 42 at 5, and for a few other hypothetically legitimate purposes. (Doc. 42 at 6). However, Mr. Titov's testimony about how Hotfile's system is used flies in the face of Hotfile's claims that it does not know what kind of files are uploaded to its system. (Titov Decl. PP 11-15, App. 4-5). The fact is Hotfile plays a "numbers game." With 240 million visits per month, it knows that a certain percentage will buy memberships. Furthermore, a large number of these memberships will be to buy speedy access to illegal content. Hotfile itself made it clear on its website that it encourages users to upload more popular content. See Doc. 17-1 and 17-2, First Amended Complaint ¶ 4.23 and Exh. F thereto. As it said on Hotfile's website: "We are trying to encourage the good promoters by increasing their earnings and to reduce the earnings for uploaders [sic] that mainly use the free hotfile [sic] resources for storage."

Although Hotfile laughably suggests that its users are using the Hotfile system to share family photo albums, this simply does not jibe with Hotfile's business model. A family photo album, even in a prolific family, would bring no more than a handful of users to the Hotfile website. Apparently Hotfile claims a 17% yield from visitors to signup. (Opp at 20.) Accordingly, it would hardly seem worth going into business for Hotfile to merely be the family photo album business. Hotfile both intends to (and does) induce widespread infringement. See Doc 17-1 ¶ 4.22, 4.23, 5.12, 5.14, and ¶¶ 10.1-10.3.

As argued in the Motion for Preliminary Injunction, Hotfile seems to place sits head in the sand with respect to infringement, and the sand may block Hotfile's eyes and ears, but it certainly does not keep Hotfile from telegraphing, loud and clear, to its army of Affiliates -- who know how the Hotfile Scheme works. Titov claims that the e-book giving users instructions on how to make money on Hotfile was authored by a third party. Doc. 43, Exh. 1, App. 8, ¶ 8. Let us accept Mr. Titov's statement as true. This would suggest greater, not less, willful blindness on Hotfile's part. If someone actually wrote a book on how to make money with Hotfile, and that person knows that Hotfile is most likely to pay its users if the users upload "new movies," and "new music," then how can Hotfile be blind to how its services are being used? Hotfile receives an estimated 240,310,078 page views per month.[6] Almost the equivalent of every man, woman, and child in America. Hotfile is the 94th most popular website on the planet.[7] Are all these people here to download powerpoint presentations? The Plaintiff has shown that this is highly unlikely.

"Willful blindness is knowledge, in copyright law as it is in the law generally." *In re Aimster Copyright Litig*., 334 F.3d 643, 650 (7th Cir. 2003) (internal citations omitted). Knowingly providing the necessary instrumentalities for infringement suffices, when coupled with a failure to take action once the knowledge of massive infringement (actual or constructive) is gained. *Metro-Goldwyn-Mayer Studios, Inc., v. Grokster Ltd.,* 380 F.3d 1154, 1163 (9th Cir. 2004), vacated on other grounds by 543 U.S. 1032 (2004); see also *Fonovisa, Inc. v. Cherry Auction, Inc.,* 76 F.3d 259, 264 (9th Cir. 1996). When the defendant should have known of the direct infringement, knowledge is properly imputed to him. *In re Aimster Copyright Litigation*, 252 F.Supp.2d 634, 653 (N.D. Ill. 2002); *Hard Rock Cafe*, 955 F.2d at 1149 (stating that "willful blindness" is equivalent to actual knowledge).

The Defendants reliance on *Perfect 10 v. Amazon.com,* 508 F.3d 1146 (9th Cir 2007) seems strange, given that a full quotation of the sentence that the defendants provide gives a virtual blueprint to the court for holding Hotfile secondarily liable in this

[6] http://www.peekstats.com/www.hotfile.com
[7] http://www.alexa.com/siteinfo/hotfile.com?p=tgraph&r=home_home

case. Under that case, a defendant materially contributes to an infringement scheme when the defendant has "actual knowledge that specific infringing material is available using its system." *Id*. at 1172. That is the case here, as the Defendant admits to receiving at least 300 takedown notices per day. (Opp. at 20.) The *Perfect 10 v. Amazon* case continues to state, directly after the above-quoted sentence, "and [the defendant] can take simple measures to prevent further damage to copyrighted works, yet continues to provide access to infringing works." *Id*. In this case, Hotfile could take simple measures. For example, if Hotfile required that uploaders provide positive identification, and checked such identification against credit card records, and then also warned uploaders that their information would be given to copyright plaintiffs, (and their credit card would be charged a penalty for uploading infringing material) this would likely scare away many of the uploaders of infringing material. Hotfile could enact a simple scheme that would take a screen grab from each file, and place an image containing an outtake from the video on its link page -- thus giving Hotfile the ability to quickly review whether it has indications of being pirated. There are myriad simple measures that Hotfile could take, but it chooses not to. If copyright thieves knew that they would be held responsible for their actions on Hotfile, or that there was no money to be made, Hotfile's traffic stream would dry up and blow away.

The availability of copyrighted material is a major draw for the Hotfile.com enterprise - otherwise it would seem unlikely that nearly a quarter of a billion people per month would visit the site. The Defendants derive revenue from Hotfile, and that revenue's level has a direct correlation to the number of users who come to the site. See *Columbia Pictures v. Gary Fung*, 2009 US Dist LEXIS 122661(C.D. Cal. 2009) at *55; *Intellectual Reserve, Inc. v. Utah Lighthouse Ministry*, Inc., 75 F.Supp. 2d 1920, 1295 n. 6 (D. Utah 1999) (finding that evidence of increased hits to a web site encouraging infringement constitutes circumstantial evidence that defendant infringed and was infringing on plaintiff's intellectual property).

IV. Plaintiff Will Suffer Irreparable Harm Without the Preliminary Injunction

Plaintiff has shown the irreparable harm being caused by Defendants' unchecked copyright infringement. See Doc. 34, Section IV(D); See also Doc. 14 ¶¶ 3-18. In order

for Plaintiff's rights to be protected and for any possible hope of justice being served, the Court must convert the TRO into a preliminary injunction.

A. The Defendants claim to stop stealing – if asked nicely.

The Defendants claim that they will stop stealing the Plaintiffs' property when asked to do so. The truth of the matter is that the Defendants do, eventually, delete specific copyright-infringing files that are brought directly to their attention by the copyright owner. In fact, it is not even permissible to flag others' intellectual property on the system. Hotfile only does so upon specific request. Doc. 43 (Titov Dec. ¶ 40, Exh. 1, App. 9). Therefore, if one of the Plaintiff's movies is uploaded twice, but the Plaintiff can only find one of the files, then the Plaintiff is powerless to remove the un-discovered file. That file remains on Hotfile, is distributed by Hotfile, and is copied again and again as Hotfile's users download it again and again. Even if the Plaintiff can find an infringing file, and the Plaintiff sends a takedown notice, Hotfile removes these files at its own leisurely pace. Hotfile has no incentive to remove them expeditiously – as even a brief delay will result in more traffic, more Hotfile memberships being sold, and more money flowing into Hotfile's coffers – all as a result of the distribution of the works of others.

B. Hotfile's Copyright Owner System is flawed

Hotfile claims that it created a special copyright owner account for the Plaintiff. (Doc. 42 at 8). This is true, but the Defendants seem to believe that this is adequate to resolve the copyright theft taking place on Hotfile. This is a deeply flawed system:

First, if the Plaintiff uses this system to delete files from Hotfile, the Plaintiff will be deleting files from Hotfile. These files are evidence in this case, both against Hotfile and against other defendants. Hotfile is quite clever in its maneuverings – granting the Plaintiff a "special copyright owner account," which would make the Plaintiff the party who destroyed the evidence – thus enlisting the Plaintiff in Hotfile's defense to do its dirty work. Once the files are deleted because of the Plaintiff's actions, the Plaintiff could hardly complain that Hotfile purged the evidence.

Second, this system continues to turn private property rights on their head. Hotfile's "special copyright owner account" is an absurd "solution" to the problem. In the Motion for Preliminary Injunction, the Plaintiff drew both factual and legal analogies

between Hotfile and the "flea market cases" in which copyright owners held flea markets responsible, when the flea markets profited from the sale of bootleg music to the flea markets' customers. If the analogy continued, this would be like the flea market owner giving copyright owners free admission to the flea market, and the right to take any bootleg content of the copyright holder that the owner could find on his own. However, the system and the metaphor both suffer from the same problem – that the stall owner would still remain free to sell other copyright infringing materials, including those of the Plaintiff, the moment that the Plaintiff turned his back. Furthermore, the system relies upon the Plaintiff being able to detect the problem in the first place by devoting its resources to prowling the internet looking for its stolen wares.

C. The MD5 system is worthless

Defendants suggest that their filtering system is an adequate solution to the rampant copyright infringement that occurs on its site. Hotfile filters content on using MD5 hash values. "An MD5 hash value is like a document's fingerprint. An algorithm creates the value by analyzing a document's content and characteristics, and assigning a unique value based on the information the document contains." Frank Vecilla, *And You May Find Yourself In a Very Large Document Review*, 27 No. 4 ACCDKT 82 (2009). Again, Defendant's plan is to shift the burden to prevent copyright infringement on hotfile.com onto the Plaintiff. Under Defendant's scheme, Plaintiffs would have to undertake the burden of creating and uploading a hash file for each of the copyrighted films content that they own and Defendant's would then "automatically" filter out matching files on their server.

While this sounds like a reasonable theory, MD5 hash filtering technology is worthless as a copyright infringement prevention countermeasure. All it does is block another file that has the precise digital fingerprint of the previously-hashed file. The digital fingerprint is easily smudged. Even "[c]hanging even one bit of data in the original input can change the hash output dramatically." Peter Bartoszek, *Deemed Distrubtion: How Talking About Music Can Violate Copyright Law*, 2008 U. Ill. J.L. Tech. & Pol'y 439, 454-55 (2009). For example, a hash file created from the collected works of Shakespeare would not be identical with the hash file created from the collected works of Shakespeare with one letter transposed. Therefore, under Defendant's proposal,

it would not be filtered. See Vecilla, supra, at 89 ("Even a very subtle difference between two documents -- for example, the addition of a dash or a period -- is enough of a variation to trigger the allocation of dissimilar MD5 hash values").

In the context of audio or video, mere variations in format or bit rate will each produce dissimilar hash values. See Bartoszek, supra, at 456. ("If a user were to search for a specific song, for example, the user may be presented with a number of different versions of the same song, each varying slightly in their bitrate. . .that would generate a different hash"). Therefore,

> [b]ecause a slight variance in the source files (such as in the ID3 tag or in the file's bitrate) would yield a different hash, this method is not reliable for discovering on a large. . . since those wishing to conceal copyrighted works could make a small change to the file and be immune from discovery. Id. at 456-57.

In fact, the ineffectiveness of MD5 hash value filtering has been noted by international courts when looking at Hotfile clones. See Oberlandesgericht [OLGZ] [Higher Regional Court of Hamburg], July 2, 2008, Az. 5 U 73/07, (F.R.G.). In a copyright infringement case involving Rapidshare (a service Defendant admits is nearly identical to their own), the Higher Regional Court of Hamburg held that MD5 filtering was wholly ineffective to prevent copyright infringement on Rapidshare.de. Id.; See also, Nate Anderson, *Achtung! RapidShare Ordered to Filter All User Uploads*, (June 24, 2009), http://arstechnica.com/tech-policy/news/2009/06/achtung-rapidshare-hit-with-24m-fine-content-filter-rules.ars (discussing the case in English).

Defendant's plan is like a fence asking you to take detailed pictures of everything in your house and if it shows up in his fencing operation, he will return it to you. But if there happens to be one smudge of dirt on your priceless Ming vase that makes it different from the picture or if he looks at it from a different angle or under a different light, he will sell it anyways.

D. Hotfile's online agreements are irrelevant

Hotfile makes much of the fact that its Terms and Conditions prohibit the uploading of copyrighted or pornographic content. (Doc. 42 page 6). However, when

one signs up for a Hotfile account, Hotfile does not even collect the subscriber's name. See http://hotfile.com/premium.html. Instead, Hotfile simply refers the user to PayPal, so that PayPal can process the user's payment. This is hardly a binding agreement, and even if it were, despite Hotfile's protestations to the contrary, it does not seem that Hotfile terminates its Affiliates who breach this agreement, as will be shown *infra*. The fact is, this agreement, like the MD5 system is merely decorative in nature—a simple ornament that Hotfile believes it can flash in order to evade liability.

E. Hotfile's Statistical Games

Hotfile claims that less than 1% of the files uploaded on a daily basis are materials that are claimed to be infringing. (Doc. 42 at 7) Simultaneously, it does not know what kind of files are uploaded to its system. (Doc. 43 Titov Decl. ¶¶ 11-15, App. 4-5); (Doc. 43 ¶¶ 13, 28, App. 5). "Only uploaders and those with whom they have shared the stored content know the content of specific uploaded files." (Doc. 42 at page 37). Which is it? Does Hotfile have data that supports its 1% claim? If so, how does it know that if it has no idea what kind of files are uploaded to its system?

Despite the clear contradiction, and lack of credibility that it suggests, let us presume arguendo that Hotfile's "1%" claim is correct. This is a clever, but transparent statistical game. Hotfile claims that 130,000 files are uploaded per day. Id. It then claims that it receives only 300 takedown notices per day. However, Hotfile does not say how many links are provided in these takedown notices.[8] Hotfile does not say how many files are deleted through its "copyright holder accounts." And, Hotfile forgets that the 300 notices it receives per day are from copyright owners who have the ability and the wherewithal to find the infringing materials, which Hotfile admits are difficult to find without assistance. See Doc. 42 at page 5. Furthermore, this 1% analysis ignores what is truly important – which files generate the most revenue, and which files are the most frequently downloaded? Hotfile clearly does not wish to encourage people to use its system for mere storage of backup files. See Doc. 17-1, FAC ¶ 4.23 and 17-2, Exh. F thereto. The reason is clear – Hotfile makes money by selling subscriptions. Those subscriptions are a "numbers game." The more traffic that comes to a particular file,

[8] For example, one of plaintiffs DMCA notices contained 800 files.

coupled with the size of that file, the more likely a user is to buy a subscription. Hotfile is a clever scheme, but cleverness is not a defense to copyright infringement.

V. Hotfile does not qualify for the DMCA's Safe Harbor

A. Hotfile's failure to list a registered agent with the U.S. Copyright Office

Hotfile admits that it did not list its registered agent with the United States Copyright Office until Dec. 24, 2009. (Doc. 42 page 38). It claims that this was due to an "inadvertent error." 17 U.S.C. § 512(c)(2) clearly provides that in order to take advantage of the DMCA's safe harbor provisions, the Defendant had to comply with its strict statutory requirements including designation of an agent, including designation of a registered agent. There is no "inadvertent error" exception. While Defendant's liability might be limited under 17 U.S.C. § 512(c)(2) if it had registered an agent with the Copyright Office, it failed to do so. Its reason for failing to take this step are immaterial, as Defendant failed to comply with the statute's plain language.

Congress' grant of immunity to any group is rare, and therefore such protections are jealously guarded by the courts. See *U.S. v. Philadelphia Nat'l Bank*, 374 U.S. 321, 348 (1963). ("Grants of immunity…should always be strictly construed." *Helvering v. Gowran*, 302 U.S. 238, 241 (1937); *Davis v. Parker*, 58 F.2d 183, 187-88 (5th Cir. 1995); *Sierra Club v. Tenn. Valley Auth*., 430 F.3d 1337, 1356 (11th Cir. 2005). (Waivers of immunity are to be strictly construed, even when it defeats a party's claim. *Sierra Club v. Tenn. Valley Auth.*, 430 F.3d 1337, 1356 (11th Cir. 2005).

Defendant has failed to comply with the registration requirements of 17 U.S.C § 51(c)(2) and therefore, the immunity provisions of § 512 should not apply to Defendant. Moreover, Defendant cannot hide behind the idea that it substantially complied with § 512(c)(2). Id. The statute's plain language states that substantial compliance is permissible only to information to be displayed on the web site and supplied to the Copyright Office. This leniency does not apply to the requirement that Defendant had to register an agent with the Copyright Office in order to have statutory immunity.

Where standards are so black-and-white, courts have applied a strict compliance rule instead of the more forgiving substantial compliance rule Defendant seeks. See *Smith v. Chapman*, 614 F.2d 968 (5th Cir. 1980) (substantial compliance with a federal law is counter to the law's purpose).

The Defendants misunderstand the DMCA's notice and takedown provisions. The Defendants state that Plaintiff's DMCA notices did not meet the requirements of the DMCA because the did not specify which specific works were associated with the recited URLs . See Opposition page 10, Section C. Defendants misunderstand because the DMCA does not privilege infringers to continue to infringe if a notice is only substantially complied with, but in fact, the notice and the takedown provision is one of the few that allows substantial compliance. When a copyright owner substantially complies, anyone seeking to take advantage of the DMCA must heed the takedown notice. However, a defective takedown notice does not grant Hotfile the privilege to continue broadcasting the infringing material.

Moreover, Defendants misstate the evidence submitted as the DMCA notices included as Doc. 43 Ex. 1-K, App. 328, include the titles and copyright registration numbers in the subject heading of the notices sent, and therefore, they do not suffer from the claimed defects.

B. Despite Defendant 's claims to the contrary, it has not terminated the accounts of every individual accused of posting infringing content.

On August 15, 2009, Plaintiff sent a DMCA takedown notice, containing the titles of the works and the copyright registration certificate numbers for the following works, "Bryan F*cks Lucas – ACM0716", "Luke and Josh – ACM0708," "Keith's Tag Team – ACM0707," "Hugh – ACM0706," and "F**king Ty – ACM0702." See Doc. 43 Exh. 1-J, App. 101. The infringements were posted by the Hotfile affiliate GXcandals.com, who is still actively posting infringing files to Hotfile.com to this date using GXcandals.com Affiliate account. See http://hotfile.com/list/295740/790eeb6.

Additionally, on Dec. 12, 2009, Plaintiff sent takedown notices regardings infringements found on www.gayup.org regarding the Hotfile.com links in Appendix A.[9]

As a result of the quantity and frequency of infringing works posted to Hotfile.com and made publicly indexed on his website, gayup.org, Defendant Dragos Badan (owner/operator of Gayup.org) was added to the present action. His account was

[9] the links are included in an Appendix hereto so that only the Appendix may be sealed as the links contain language that could be deemed vulgar

not terminated by Hotfile.com; it was through his own volition after being informed of the present action that he terminated his website on or around Jan. 25, 2010. The Defendant has not even terminated the accounts of all Defendants in this action, let alone all other infringing affiliates.

C. <u>The Defendants Claim that if a private property owner doesn't lock up his property enough, it is not the thief's fault if he can't resist the temptation.</u>

The Defendants seem to believe that since the Plaintiff does not use its technology to stop others from stealing its content, that the Plaintiff is itself at fault – or even that the Plaintiff is trying to "entrap" others into stealing its content. (Doc. 42 at 9) The Defendants claim that since the Plaintiff does not employ Digital Rights Management technology ("DRM"), that it is at fault for the Plaintiff's theft. This argument is without merit. A thief may not defend himself by claiming that his victim should have chained down his property. As the Defendant's own Exh. shows, Liberty's motive for removing file based DRM protection was that it is widely-recognized that DRM is ineffective in the fight to control piracy. (Doc. 42 Exh. 2-B, App. 441). See, also Scott Monkman, *Corporate Erosion of Fair Use: Global Copyright Law Regarding File Sharing*, 6 ASPER REV. INT'L BUS. & TRADE L. 265, 284 (2006) (discussing the ineffectiveness of Digital Rights Management technology and calling for content providers to abandon it); Bill Herman, *Breaking and Entering my own Computer: The Contest of Copyright Metaphors*, 13 COMM. L. & POL'Y 231 ("DRM-based encryption is an inherently leaky solution.); Fred von Lohmann, *Measuring the Digital Millennium Copyright Act Against the Darknet: Implications for the Regulation of Technological Protection Measures*, 24 LOY. L.A. ENT. L. REV. 635, 640-41 (2004) (noting that technological solutions to copyright infringement have proven ineffective).

In fact, one of the nation's leading minds on the subject concluded that DRM technology is actually counterproductive in the fight against piracy. See Fred von Lohmann, *Digital Rights Management: The Skeptics' View*, ELECTRONIC FRONTIER FOUNDATION.[10] ("DRM may be part of the problem, pushing frustrated consumers into the arms of unauthorized channels like Kazaa."); c.f. David Choi, *Spotlight on*

[10] *found at* http://www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf (last visited Nov. 15, 2005)

Intellectual Property Law, The Ineffectiveness of DRM, 51 ORANGE COUNTY LAWYER 14 ("DRM has proven not only to be ineffective to the copyright holder but has had a deleterious effect on the consumer.").

Ernest Miller, a respected author on copyright issues said it best:

> [N]o one goes around claiming that physical locks stop burglary. Everyone recognizes that it isn't the lock that does the work, but the law. Any reasonably competent crook can bypass most security systems. If they don't it is because of law, not the physical aspects of the lock.[11]

Unfortunately, Hotfile seems to believe that it is locks, and not laws, that should be employed to protect private property rights. This court should educate the Defendants to the contrary.

Even if the Defendant's claim were true, that the robbed party can not complain if he did not adequately weigh down his property, the Plaintiff has engaged in an agreement to manage its digital rights - however, it has only agreed to do so with a program that provides effective digital fingerprinting technology. As discussed *supra*, the Defendant's "window dressing" technology is useless for video files - and only marginally useful for music files.

VI. Civil Conspiracy

Plaintiff also brings a civil conspiracy claim against Defendant. The elements of this claim are: 1) two or more persons or entities; 2) an object to be accomplished; 3) a meeting of the minds on the object or course of action; 4) one or more unlawful, overt acts; and5) damages as a proximate result. *Chron Tri v. J.T.T.*, 162 S.W.3d 552, 556 (Tex. 2005); *See also Operation Rescue-Nat'l v. Planned Parenthood*, 975 S.W.2d 546, 553 (Tex. 1998); *Schlumberger Well Surveying Corp. v. Nortex Oil & Gas Corp.*, 435 S.W.2d 854, 856 (Tex. 1968). They are present in this case.

In this case, two or more entities are present. The conspirator's object must be to either have "an unlawful purpose or…accomplish a lawful purpose by unlawful means." *Triplex Commc'ns, Inc. v. Riley*, 900 S.W.2d 716, 719-20 (Tex. 1995); *Massey v. Amoco*

[11] Ernest Miller, Prove DRM Works: Eliminate the DMCA *found at* http://importance.corante.com/archives/004619.html (June 28, 2004) (last visited February 6, 2010).

Steel Co., 652 S.W.2d 932, 934 (Tex. 1983). In this case, the conspiracy had one purpose coated with several facets of illegal conduct.

The "meeting of the minds" required to prove a conspiracy, *Chron Tri*, 162 S.W.2d at 556, is an evidentiary question. *See March Madness Athletic Ass'n LLC v. Netfire Inc.*, 120 Fed. Appx. 540, 546 (5th Cir. 2005) (holding that plaintiffs could not establish a meeting of the minds without evidence that the parties were working toward a common goal); *Salinas v. Univ. of Tex.-Pan Am.*, 74 Fed. Appx. 311, 314-15 (5th Cir. 2003). In this case, the evidence adduced so far shows that each conspirator acted to upload copyrighted content for profits in which they all shared. This information, however, goes to show that each party shared this common goal, satisfying this requirement of a civil conspiracy.

International Paper Company v. Frame, 67 Fed. App. 251 the company was able to prove numerous showing circumstantial evidence of conspiracy. 67 Fed. Appx. 251, No. 01-41094 *2003 WL 21195497* at 4 (5th Cir. 2003). In this case, Plaintiff can point to dozens of instances where Defendant uploaded content for others to download. These discrete actions, analogous to those in *International Paper*, coalesce into a conspiracy to deprive Plaintiff of proceeds it rightly deserves from the consumption of its creations. *International Paper Company,* 67 Fed. Appx. 251 2003 WL 21195497;

There can be no real question that the pecuniary harm Plaintiff suffered from Defendants' unauthorized distribution of its content are damages proximately caused by this conspiracy. In *Metro-Goldwyn-Mayer Studios Incorporated v. Grokster, Limited*, MGM sought damages for the repeated uploading and sharing of its copyrighted material by Grokster, for which MGM had a viable claim for damages. 545 U.S. 913 (2005). *See Veeck v. S. Bldg. Code Cong. Int'l, Inc.*, 293 F.3d 791, 825 (5th Cir. 2002) (authorizing the recovery of damages where guilty party had infringed copyrights).

VII. The Plaintiff's Alter Ego Claim Passes

The Defendants claim that the Plaintiff's Alter Ego claim fails because Mr. Titov maintains adequate separation from Hotfile corp. As the Defendant states, if a failure to disregard the separate identities would result in fraud or injustice, the Alter Ego claim would not fail. See, e.g., *Richards Group, Inc. v. Brock*, 2008 U.S. Dist. LEXIS 55139 (N.D. Tex. July 18, 2008) ("A corporation's separate identity may be disregarded or

'pierced,' however, upon a showing that it is a sham or a dummy or where necessary to accomplish justice."(citing *Oceanics Schools, Inc. v. Barbour*, 112 S.W.3d 135, 140 (Tenn. Ct. App. 2003)). Although there is a laundry list of factors, no factor is key. See *United States v. Jon-T Chemicals, Inc*., 768 F.2d 686 (5th Cir. Tex. 1985).

In this case, Mr. Titov shows but the hallmarks of being an alter ego of Hotfile corp. Mr. Titov claims that Hotfile maintains corporate formalities. (Doc. 43 Exh. 1, App. 3 ¶ 4) . However, Mr. Titov does not tell us what qualifies him to make conclusory legal statements about Panamanian law. Hotfile does not maintain the corporate formality of maintaining a valid registered agent in Panama. See Doc. 26 ¶¶ 3-4 and Exh.s A, B, and C thereto. Panamanian law requires that all Panamanian Corporations provide the name and domicile of the corporation's registered agent in the Republic of Panama. See Corp. Law of Panama, N° 32 of February 26, 1927, Ch. I, Art. 2(7). Accordingly, it is consistent with Hotfile's illegal nature that it would seek to avoid the one Panamanian corporate requirement that might otherwise make service of process a bit less burdensome. While this may seem to be "mere paperwork" to Hotfile, since Hotfile's key defense to date has been t.

Mr. Titov's claims that Hotfile's finances are separate from his own. (Doc. 43 Exh. 1, App. 3 ¶ 7). However, if one purchases a Hotfile.com membership, the money seems to go directly into Mr. Titov's bank account. See Doc. 16-1 Exh. E; See also Doc. 26 Exh. E. Titov's protestations are not supported by the evidence in the record.

VII. The Injunctive Relief Is Reasonable

The injunctive relief granted so far has required that the Defendant stop breaking the law, and that the Defendant not take its ill-gotten gains to some far-flung jurisdiction – thus rendering relief impossible. The Defendant argues that the injunction should, if issued, be limited to "requiring Hotfile to remove and add to its filter files that have been specifically identified by Plaintiff within a reasonable period of time." (Doc. 42 page 40). In other words, the Defendant wants the Court to order it to simply motor along, infringing upon the Plaintiff's rights – but, if the Plaintiff wishes to continue to devote its resources to tracking down the hard-to-find infringements, the Defendant will agree to take them down upon specific request. Additionally, the Defendant will add the materials to its filter,which it identifies as MD5/SHA1 "digital fingerprinting technology." The

problem is, that this is worthless technology. See Oberlandesgericht [OLGZ] [Higher Regional Court of Hamburg], July 2, 2008, Az. 5 U 73/07, (F.R.G.). See also, Nate Anderson, *Achtung! RapidShare Ordered to Filter All User Uploads*, (June 24, 2009), http://arstechnica.com/tech-policy/news/2009/06/achtung-rapidshare-hit-with-24m-fine-content-filter-rules.ars.

Defendant throws a veritable tantrum over a comment made by counsel for the Plaintiff, that one of the Plaintiff's goals is to "put Hotfile out of business." This is a legitimate goal. Hotfile has stolen millions of dollars from the Plaintiff and other copyright owners. If Hotfile cannot operate lawfully and profitably the the profit must yield to the law. See, e.g. *Playboy Enters. v Webworld*, 968 F. Supp. @ 1175. ("If a business cannot be operated within the bounds of the Copyright Act, then perhaps the question of its legitimate existence needs to be addressed.")

Proving irreparable harm generally is not required in copyright litigation, and presumed once the moving party has established a case of copyright infringement. *MyWebGrocer, LLC v. Hometown Info, Inc*., 375 F.3d 190, 193 (2d Cir. 2004) (noting that when a copyright plaintiff makes a prima facie showing of infringement, irreparable harm may be presumed); *Elvis Presley Ents., Inc. v. Passport Video*, 349 F.3d 622, 627 (9th Cir. 2003); *Vault Corp. v. Quaid Software Ltd*., 655 F.Supp 750, 756 (E.D. La. 1987); *E.F. Johnson Co. v. Uniden Corp. of America*, 623 F.Supp 1485, 1491 (D. Minn. 1985); *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522, 533 (6th Cir. 2004). Every day, more and more of the Plaintiffs works are being broadcasted on Hotfile. The Defendant clearly will not take any meaningful steps to stop unless a court forces it to.

This court has rightly ordered the Defendant to stop infringing on the Plaintiff's works, and the Plaintiff should therefore either shut itself down, or adapt its business model to be fully protective of others' intellectual property rights. Indeed, it is not just the Plaintiff's works that are being stolen on Hotfile, as the Plaintiff has already demonstrated by suggesting a simple Google search for the name of any movie, and the words "hotfile.com." Such a result will show what a bonanza of stolen material resides

on the Hotfile system. [12]

The Defendant could take a number of steps to mitigate the harm that its system causes to intellectual property owners, and while some ideas have been suggested, the Defendant could likely take mightily effective steps -- if only it were willing to. The Defendant's suggestion, that it should be able to use MD5/SHA1 fingerprinting technology should be roundly rejected, as this method of preventing piracy has been proven to be worthless. The Defendant's claim that a piracy report would create a "hash file" that would stop similar works from being uploaded is, a gross falsehood - and the evidence shows that. At the genesis of this dispute, approximately 800 individual works were the subject of a DMCA takedown notice. The Plaintiff then found duplicates of these movies, time and again, on the Hotfile system. MD5/SHA1 is not just a leaky sieve, it is like using a chain link fence to keep out the rain.

The Plaintiff hardly "obfuscates the fact that Hotfile has removed every file that Plaintiff has ever identified as infringing." (Opp. at 30). In fact, Plaintiff hereby stipulates that all files that are a) found by the Plaintiff, and b) are reported to the Defendant, are eventually deleted. They may even be added as the MD5 list (however Defendant has not provided evidence of this). But even if they were added, this has been shown to be no remedy at all. However, it would be no defense for a pawn broker, whose business depends on stolen goods, to simply agree to return goods to victims who walk in the front door with a photo of their goods, while he continues to receive truckloads of stolen goods in through the loading dock. That is what Hotfile does

With respect to Hotfile's claim that the injunctive relief regarding Hotfile's assets would put it out of business, or render it unable to pay for representation, this is clearly not the case. Hotfile has dozens of resellers. See http://hotfile.com/resellers.html. While they have been named as defendants, and the Plaintiff asked that the Court freeze their accounts too, the Court declined to do so. Clearly, since Hotfile has neither ceased

[12] The Defendant incorrectly concludes that the Plaintiff thinks that Hotfile must regularly patrol Google for works on its system. (Opp. at 17). This would be a reasonable task, as one employee could be paid at Bulgarian wages to do so, and this would presumably not cause too much burden on Hotfile - meanwhile, it would likely create quite a dent in the Hotfile infringement problem. However, Plaintiff does not demand this, but rather points to the relative ease of finding pirated material on Hotfile as clear evidence of Hotfile's willful blindness.

operations, even slowed down in its massive infringement marathon, these resellers seem to be doing their jobs effectively. Hotfile's frozen assets represent a mere fraction of its assets - but they represent the only assets that this court has decided to place under its control. It is certain that the expensive lawyers hired by Hotfile are not doing this out of charity, and they certainly cannot be doing this to have a chance at accessing the small amount of money in the Defendant's PayPal account.

The Public Interest hardly favors Hotfile, and its arguments in that respect are thin - at best. The only thing that the public uses Hotfile for is to steal intellectual property from American companies. The Defendant claims that it should be protected by the DMCA. (Opp. at 31), but it has already been shown that the Defendant is entitled to no safe harbor under the DMCA.

The TRO should be converted to a Preliminary Injunction. If the Order is to be modified at all, it should be expanded so that the "Hotfile Resellers'" US assets will be frozen as well. Furthermore, if Hotfile continues to infringe upon the Plaintiff's works, Hotfile should be held in contempt and should be fined. It is quite clear that if this Court does agree to fine Hotfile for each infringement brought to the court's attention, Hotfile and its team of technicians will likely fashion a technological remedy - once they are economically persuaded to do so. The effectiveness of their ingenuity will likely be commensurate with the financial motivation that this Court gives them. Accordingly, it is the Plaintiff's request that this Court impose a penalty of at least $10,000 per infringement that is found after February 9, 2010. If it does so, the Plaintiff is confident that Hotfile will either miraculously solve the problem, or perhaps this court will find what it found in 1997 -- that some business models, if incapable of lawful activity, should possibly be shut down altogether. *Playboy Enters. v Webworld*, 968 F. Supp. @ 1175.

Respectfully submitted,

s/ Marc Randazza

LEAD COUNSEL:
Marc J. Randazza, Esq.
302 Washington Street, Suite 321
San Diego, CA 92103

s/Gary Krupkin

LOCAL COUNSEL:
Gary P. Krupkin, Esq.
1116 Commerce Drive
Richardson, Texas 75081

Telephone:619-866-5975
Facsimile: 619-866-5976
Electronic Mail: marc@corbinfisher.com
Massachusetts Bar Card No.: 651477
Florida Bar Card No.: 625566
Admitted to practice before the
United States District Court
Northern District of Texas

Telephone: 972-261-8284
Facsimile: 972-671-3671
ElectronicMail:krupkinlaw@gmail.com
Texas Bar Card No.: 00790010
Admitted to practice before the
United States District Court
Northern District of Texas

CERTIFICATE OF SERVICE

This is to certify that on the 8th day of February 2010, a true and correct copy of the foregoing document has been served via CM/ECF notification, as well as email service.

s/ Marc Randazza