UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
MIAMI DIVISION

DISNEY ENTERPRISES, INC., TWENTIETH CENTURY FOX FILM CORPORATION, UNIVERSAL CITY STUDIOS PRODUCTIONS LLLP, COLUMBIA PICTURES INDUSTRIES, INC., and WARNER BROS. ENTERTAINMENT INC., *Plaintiffs*, vs. HOTFILE CORP., ANTON TITOV, and DOES 1-10. *Defendants*.	Case No. 1:11-cv-20427-UU

MEMORANDUM OF LAW IN SUPPORT OF PLAINTIFFS' EMERGENCY MOTION FOR AN ORDER PROHIBITING SPOLIATION AND TO PRESERVE EVIDENCE

Plaintiffs respectfully seek an order (i) requiring defendants to preserve evidence that is vital to this action and (ii) permitting plaintiffs limited immediate discovery to take possession of copies of crucial electronic data that are particularly vulnerable to alteration and spoliation. Plaintiffs bring this motion on an emergency basis, *inter alia*, on account of defendants' actions over this past holiday weekend and the credible risk that, absent urgent Court intervention, important categories of evidence may be permanently lost. Plaintiffs have given defendants' counsel notice of this motion and propose an accelerated briefing schedule so as to afford defendants an opportunity to be heard.

Since shortly after filing this action, plaintiffs' counsel have been conferring with defendants' counsel concerning the relief requested in this motion. While defendants' counsel indicated that defendants would commit to preserve some categories of documents, defendants affirmatively refused to commit to preserve other highly relevant categories. Moreover, defendants' professed agreement to preserve any evidence proved illusory, as defendants refused to enter into a written stipulation that might be presented to this Court. Declaration of Duane C. Pozza, dated Feb. 22, 2011 ("Pozza Decl.") ¶¶ 3-4. Following those discussions, and following days of "radio silence" from defendants and their counsel, over the holiday weekend defendants began making dramatic changes to their business practices that raise grave concerns that defendants are in fact attempting to alter or despoil crucial electronic evidence. Pozza Decl. ¶ 6. Accordingly, plaintiffs bring this emergency motion, on the following bases:

First, defendants Hotfile Corp. and Anton Titov ("defendants") operate a website at www.hotfile.com ("Hotfile") that is a hub for massive copyright infringement, including of plaintiffs' copyrighted motion pictures and television programs. In short, defendants pay users to upload to Hotfile's computer servers "popular" content, which is almost invariably copyright

infringing, so that defendants can charge other users to access and download those infringing works. That is defendants' entire business model and there is nothing legitimate about it.

Indeed, the very nature of defendants and their operation further reveal the risk of spoliation. Defendants do not behave like any legitimate business, but rather operate in the shadows. They conceal their identities and whereabouts through offshore entities, fictitious addresses, mail drop services, and at least one known shell company. Defendants are cagey even about who runs Hotfile: defendants' website claims that a Panamanian corporation is the operator of Hotfile; yet, in a separate litigation, defendant Titov claimed that Hotfile conducted business through a Bulgarian company. Defendant Titov is similarly unscrupulous: To contest service of process in another case, he submitted sworn testimony claiming that he is located in Bulgaria. In fact, however, Titov has a residence in Florida, from where he operates both Hotfile and Hotfile's internet service provider, which is a Florida-registered company. *Infra* at 8-9.

Second, the nature of the evidence itself makes it particularly vulnerable to spoliation. Most of the key evidence in this case is in electronic form, entirely under defendants' control, and subject to quick and easy deletion that would render it irretrievable. Hotfile's users upload and download a vast store of infringing content files to and from defendants' servers, and defendants possess records of such activity. Defendants are thus in the sole possession of the key electronic evidence that will demonstrate the unlawful reproduction and distribution of plaintiffs' copyrighted works. Clearly, defendants have a powerful interest in preventing that data from seeing the light of day. *Infra* at 7-8.

Third, defendants have violated their obligation to preserve evidence in connection with other litigation. Other copyright owners sued defendants as early as late 2009. Yet, Hotfile maintained its public policy of automatically deleting content files after a period of time;

defendants also continued to permit Hotfile's users – some of them likely commercial enterprises engaged in criminal copyright infringement – to delete uploaded content files. Those content files and the associated data about their downloads are critical evidence of infringement. Most recently, over the just-concluded holiday weekend, there were press accounts (and user reports) of defendants deactivating the accounts of infringing users en masse – a dramatic change in defendants' business practices – raising serious concerns about the preservation of that highly incriminating evidence. *Infra* at 12-14.

Fourth, although defendants' conduct standing alone more than sufficiently justifies the requested relief, the controlling authorities permit the Court to take into account the historic conduct of similarly situated online infringement defendants – and that history confirms the grave risk of evidence spoliation. As documented below, in recent years online piracy defendants have shown time and time again that they will delete or alter the most incriminating electronic data given the opportunity. This type of spoliation can lead to years of litigation and sanctions awards, while depriving plaintiffs of critical evidence in the case. *Infra* at 10-12.

Finally, the requested relief will not unduly burden defendants. Defendants business requires them to store enormous quantities of data. The preservation of evidence to meet their litigation obligations cannot credibly be claimed to burden defendants. Moreover, through the requested discovery, plaintiffs have offered to eliminate any inconvenience. Plaintiffs advised defendants that plaintiffs would stipulate to relieve defendants of their obligation to preserve content files after plaintiffs obtained discovery allowing them to secure a small representative sample of files, which could be accomplished quickly and with minimal burden to defendants. Defendants refused. *Infra* at 13-14, 18-20.

Each of these considerations supports emergency relief targeted to ensure that critical

evidence is preserved. Specifically, plaintiffs respectfully request that the Court order defendants to preserve categories of electronic data that will bear directly on the outcome of this case, including all registered user data, user upload and download data, communications with users and defendants' so-called "Affiliate" partners, business and marketing plans and internal communications about Hotfile's business, and content files and associated data. Plaintiffs further request leave to take immediate discovery to obtain copies of data related to Hotfile-distributed content files so that plaintiffs may design a protocol to select a representative sample of those particularly vulnerable files. The requested relief is reasonable and targeted at identified categories of electronic information that is at risk of spoliation and which, in comparable infringement cases, has in fact been destroyed. The requested relief is also more limited than that approved by this Court in *Dell Inc. v. BelgiumDomains, LLC*, No. Civ. 07-22674, 2007 WL 6862341 (S.D. Fla. Nov. 21, 2007), which authorized the seizure of evidence and expedited discovery of defendants and third parties in light of the risk of evidentiary spoliation.

I. BACKGROUND

A. Operation of Hotfile.

Defendants are engaged in the infringement of plaintiffs' copyrighted motion picture and television properties on a massive scale. Defendants carry out their theft of plaintiffs' works through the operation of Hotfile, an online hub for distributing popular entertainment content without authorization, including hundreds of thousands of copies of plaintiffs' copyrighted works. Compl. ¶ 1. Hotfile makes money by selling users "Premium" subscriptions that allow downloading users quick and easy access to this infringing content. Compl. ¶ 24.

To ensure an unending supply of popular copyrighted content, Hotfile actually pays users to upload popular files, which are overwhelmingly copyright infringing entertainment properties. Defendants thus actively encourage their users to upload to defendants' computer servers

infringing copies of the most popular entertainment content in the world today. Once uploaded, defendants provide their users a "link" to the infringing content on Hotfile's servers, which users then share with others, who can download the content by clicking the link. Defendants encourage their users to widely disseminate these "links" on public websites and other internet locations so that as many people as possible will locate the links and use them to download the infringing content from defendants' servers. Defendants pay uploading users more depending upon how many times the infringing content is downloaded by others – the more frequently the content is downloaded illegally, the more defendants pay the uploading user. Defendants also pay the pirate websites that host and promote "links" to infringing content on defendants' servers. Compl. ¶¶ 2, 28-34.

Defendants profit handsomely from this copyright infringement by charging a monthly fee to users who wish to download content from defendants' servers. In other words, defendants pay people to put infringing copies of plaintiffs' popular works on their computer servers, and then use the lure of those copyrighted works (and the copyrighted works of others) to entice users to pay defendants for the privilege of accessing and downloading the works from defendants' computer servers. That is defendants' entire business model. Compl. ¶¶ 24-27.

Defendants make no bones about the fact that they are in the business of distributing content they do not own. They pay users only for uploading the most popular files (*i.e.*, copyrighted entertainment content) and only if those files are downloaded by *thousands* of defendants' other users. In fact, defendants have cautioned users to "[u]pload files only if you intent [sic] to promote them" by posting links to the files on public websites. Pozza Ex. G. Defendants go so far as to penalize uploading users if their uploaded files are not downloaded in sufficient volume, explaining that the purpose of Hotfile's compensation scheme is "to

encourage the good promoters by increasing their earnings and to reduce the earnings for uploaders that mainly use the free hotfile resources for storage." Pozza Ex. H.

B. Defendants Are Liable for the Rampant Infringement On Hotfile.

Defendants are directly liable for the infringement of plaintiffs' copyrighted works because they distribute and transmit copies of those works to downloading users without authorization. *See Cable/Home Commc'n Corp. v. Network Prods., Inc.*, 902 F.2d 829, 843 (11th Cir. 1990); *Arista Records LLC v. Usenet.com, Inc.*, 633 F. Supp. 2d 124, 146-49 (S.D.N.Y. 2009) ("*Usenet II*"); *Playboy Enters., Inc. v. Webbworld, Inc.*, 968 F. Supp. 1171, 1175 (N.D. Tex. 1997), *aff'd* 168 F.3d 486 (5th Cir. 1999) (per curiam); Compl. ¶ 49.

Defendants also are secondarily liable for the rampant infringement on Hotfile. First, as evidenced through their conduct and expression, defendants operate Hotfile with the object that the system be used by Hotfile users for widespread copyright infringement. They are thus liable for inducement of infringement, under *Metro-Goldwyn Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005). Compl. ¶ 60. Second, defendants materially contribute to their users' infringement with full knowledge that the Hotfile system is being used overwhelmingly for copyright infringement. Defendants are thus contributorily liable for infringement. *See Cable/Home*, 902 F.2d at 845 ("This court has stated the well-settled test for a contributory infringer as 'one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another.'") (quoting *Gershwin Publ'g Corp. v. Columbia Artists Mgmt. Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971)); Compl. ¶ 61. Third, defendants derive a substantial financial benefit from their users' copyright infringement while declining to exercise their right and ability to mitigate that infringing activity. They thus are vicariously liable for infringement. *See BUC Int'l Corp. v. Int'l Yacht Council Ltd.*, 489 F.3d 1129, 1138 n.19 (11th Cir. 2007); Compl. ¶ 62.

C. There is a Serious Risk of Spoliation of Critical Electronic Evidence.

1. *Defendants Possess Easily Deleted Electronic Evidence That Documents Their Massive Online Infringement.*

Evidence necessarily generated by defendants' system is electronic, entirely within defendants' control, and subject to quick and easy deletion by defendants – who have every incentive to ensure it never sees the light of day. *Dell*, 2007 WL 6862341, at *1. This evidence is highly subject to quick spoliation because it is stored electronically, and may be rendered irretrievable absent Court action. Explaining the particular utility of expedited discovery in online copyright infringement actions, Moore's Federal Practice notes that "evidence [] ***can easily be deleted*** in actions involving illegal trade of music and video files posted on the internet." *7 James Wm. Moore, et al., Moore's Federal Practice* ¶ 37A-23 (3d ed. 1999) (emphasis added). Indeed, this Court recognizes that evidence in "electronic form [is] subject to quick, easy, untraceable destruction." *Dell*, 2007 WL 6862341, at *2; *see also Arista Records LLC v. Usenet.com, Inc.*, 608 F. Supp. 2d 409, 434 (S.D.N.Y. 2009) ("*Usenet*") (critical electronic evidence destroyed by permitting it to expire off purposefully reconfigured computer servers).

As fully detailed in the accompanying Declaration of Ian Foster, Distinguished Service Professor of Computer Science at the University of Chicago, for Hotfile to operate the way it does, defendants must maintain a variety of electronic data, including: (a) the infringing content files defendants distribute from their servers (*e.g.*, a video file containing part or all of a major motion picture); (b) content reference data (*i.e.*, key information relating to each content file, including its "link" and unique Hotfile identifier); (c) user data, including records of payments to users for downloads of their uploaded content; and (d) activity data (*i.e.*, information showing downloads and uploads of files). *See* Declaration of Ian Foster ("Foster Decl."), ¶¶ 6-14.

As explained more fully *infra* at Section II, this evidence is critical to showing that defendants and their users directly infringed plaintiffs' copyrights by unlawfully distributing copies of plaintiffs' copyrighted works, *see Usenet*, 608 F. Supp. 2d at 440; that an overwhelming percentage of content stored on and downloaded from defendants' system is infringing, which is highly relevant to showing that defendants induce infringement under the Supreme Court's decision in *Grokster*, 545 U.S. at 922, 940; that defendants had actual or constructive knowledge of the infringement taking place on their system and materially contributed to it, making them contributorily liable, *see Usenet*, 608 F. Supp. 2d at 440; and that defendants received a direct financial benefit from that infringement and declined to exercise their right and ability to supervise it, making them vicariously liable, *see id*.

2. *Defendants Operate in the Shadows Unlike Legitimate Businesses.*

Defendants appear to operate and support Hotfile using a maze of corporate entities, some set up offshore, that hide behind fictitious addresses and proxies to conceal their true whereabouts and operators. They are not doing business as legitimate corporate entities, and have created at least one known shell corporation to shield their infringing operations already.

Hotfile Corp., for example, purports to be a Panamanian corporation. It identifies an address in Panama on the Hotfile website, but Hotfile Corp. has no observable presence at that address. *See* Pozza Ex. I at 7. In another lawsuit brought by unrelated copyright holders, defendants claimed that Hotfile Corp.'s principal place of business was actually somewhere in Bulgaria, which, as discussed below, plainly is not true. *See* Pozza Ex. J at 3, 7. Moreover, although the Hotfile website identifies the Panamanian company "Hotfile Corp." as its operator, in yet another lawsuit, Titov has claimed that it was a Bulgarian company named "Hotfile, Ltd." that contracted to provide web hosting services for the Hotfile website. Pozza Ex. K at ¶¶ 5, 7.

Titov is a manager and shareholder of Hotfile Corp., and he claims to be a Russian citizen

and a resident of Bulgaria, who must be served in Bulgaria because his business operations are located there. *See* Pozza Ex. J at 3-4, 7. However, Titov is residing and doing business in the United States – in Florida – from which he operates Hotfile; Titov separately operates another Florida corporation, Lemuria Communications, Inc., of which he is the President, majority shareholder and sole officer and director, from Florida. *See* Pozza Decl. ¶ 22; Ex. J at 4, n.1; Ex. K at ¶ 3; Ex. L. Lemuria, in turn, is a shell company run by Titov that was founded for the sole purpose of providing web-hosting services to Hotfile. Pozza Ex. K at ¶ 5. Titov appears to have established Lemuria to shield Hotfile from the actions of legitimate internet service providers, which would be required to terminate customers, such as Hotfile, that are repeat copyright infringers. *See* 17 U.S.C. § 512(i) (addressing termination of repeat infringers). Lemuria appears to have no other customers for its internet services, *see* Foster Decl. ¶ 16; it was originally registered to a mail drop box; and its corporate filings list a Bulgarian address for Titov, notwithstanding that Lemuria is a registered Florida corporation. Pozza Decl. ¶ 13; Exs. M-N.

In short, the defendants are attempting to conceal their activities by using non-operational addresses, claiming to be operating abroad while in fact doing business in the U.S., and using shell corporations and mail drop services to shield their activities. This is not the *modus operandi* of a legitimate operation and lends fuel to the risk that defendants will despoil key evidence.

3. *Comparable Online Infringers Routinely Delete As Much Evidence As Possible Before Copyright Owners Can Use It Against Them.*

Defendants' efforts to hide their activities from view are consistent with the actions of numerous prior online piracy defendants, who have an incentive and the expertise to simply overwrite or discard electronic data – particularly the data that is most incriminating – and do

just that. Seeking to escape liability, it has become commonplace for defendants to destroy critical evidence in online infringement actions, flaunting the integrity of the judicial process and frustrating plaintiffs' efforts to seek redress for the rampant theft of their intellectual property. This Court may properly consider that history when evaluating the risk of spoliation by defendants. *See AT&T Broadband v. Tech Commc'ns, Inc.*, 381 F.3d 1309, 1319 (11th Cir. 2004); *Dell*, 2007 WL 6862341, at *2-*3. Indeed, Congress has recognized that "copyright pirates who have been sued [may have] a window of opportunity to destroy evidence" and has enacted legislation permitting district courts to impound infringing copies, means of copying, and associated records. H.R. Rep. No. 110-617, at 24 (2008); *see also* 17 U.S.C. § 503.

Defendants follow in a long line of notorious online infringers who have engaged in similar conduct. To take just two high-profile examples, the defendants in both the *Bunnell* and *Usenet.com* cases deliberately destroyed considerable amounts of electronic evidence during the discovery period and attempted to cover up their actions, leading to protracted litigation over discovery and, eventually, the imposition of sanctions, as plaintiffs never received data that was central to their case. In *Columbia Pictures Indus., Inc. v. Bunnell*, No. 2:06-cv-01093 FMC-JCx, 2007 WL 4877701 (C.D. Cal. Dec. 13, 2007) ("*Bunnell*"), the defendants, *inter alia*, modified user postings that referred to copyrighted works, changing them to refer to more innocuous items, and removed "a directory of [files] available for download, which included [hundreds of] entries for major television shows." *Id.* at *1-*2. The defendants erased some posts entirely, all to "'*clean up' the site in response to the lawsuit*." *Id.* at *2 (emphasis added). But for the testimony of defendants' third-party associates instructed to carry out the spoliation, plaintiffs might not ever have been able to prove the extent of defendants' evidence destruction. Ultimately, the Court had no choice but to impose terminating sanctions for defendants' willful

spoliation of evidence.

Similarly, in *Usenet*, the defendants destroyed evidence "[o]n the very day [they] agreed to produce [it] to Plaintiffs," and "engaged in a calculated reconfiguration of their servers" which caused infringing files to "expire[] off the system almost immediately." 608 F. Supp. 2d at 434, 436. Defendants then "ma[d]e sure the deleted files would be written-over and thus irretrievable." *Id*. at 436 The defendants later "wiped" key evidence from hard drives, and then tried to cover up those facts. *Usenet II*, 633 F. Supp. 2d at 135-36. The Court was forced to impose sanctions for this evidentiary spoliation – but only after lengthy discovery and motion practice to uncover defendants' destruction of this electronic evidence.

These two illustrations are just the tip of the iceberg of what has become *modus operandi* for online infringers like the defendants. *See, e.g.*, *Motown Record Co., LP v. DePietro*, No. 04-CV-2246, 2007 WL 576284, at *1 (E.D. Pa. Feb. 16, 2007) ("[d]efendant disposed of the computer allegedly used for the infringement by setting it out for trash collection"); *Atlantic Recording Corp. v. Howell*, No. CV-06-02076-PHX-NVW, 2008 WL 4080008, at *2-*3 (D. Ariz. Aug. 29, 2008) (imposing terminations sanctions for wiping of hard drive); *Arista Records, L.L.C. v. Tschirhart*, 241 F.R.D. 462, 466 (W.D. Tex. 2006) (imposing terminating sanctions where defendant destroyed electronic evidence); *Interscope Records v. Leadbetter*, No. C05-1149-MFP-RSL, 2007 WL 1217705, at *7 (W.D. Wash. Apr. 23, 2007) ("defendant destroyed the VPR Matrix hard drive even after 'skimming' the January 20, 2005 letter informing his mother that she had been sued for copyright infringement and to preserve evidence"); *In re Napster Inc. Copyright Litigation*, 462 F. Supp. 2d 1060, 1070-71 (N.D. Cal. 2006) (court imposed sanctions against defendant for deleting documents and communications); *Paramount Pictures Corp. v. Davis*, 234 F.R.D. 102, 111 (E.D. Pa. 2005) (court imposed spoliation

inference sanction on the defendant who had "wiped the hard drive clean").

The lesson of *Bunnell*, *Usenet* and the others is that rampant online copyright infringers like defendants will – if given any latitude – destroy with the click of a button damaging electronic evidence that is entirely within their control. Moreover, the kind of sophisticated defendants here, who manage large volumes of electronic data, are in a unique position to attempt to hide their tracks by selectively discarding portions of the data. Litigating such issues can stretch these cases on through *years* of unnecessary discovery proceedings, and the data may never be recovered notwithstanding plaintiffs' best efforts.

4. *Defendants' Own Statements and Actions Demonstrate A Risk of Spoliation.*

Defendants' own statements demonstrate the substantial risk of ongoing and serious evidence destruction here. Defendants' previous Terms of Service made clear that Hotfile deletes registered user information: "Hotfile ***undertakes to delete*** the client's information after completing a period of validity in the present Agreement." Pozza Ex. O (TOS) (emphasis added). And defendants currently state on their website that content files are automatically deleted from their servers, in the "Frequently Asked Questions" ("FAQ") portion of defendants' website:

> Q. For how long are files stored?
>
> A. In principle, we host data without a time limit. ***But files that have not been accessed for 90 days are deleted to relieve the system of forgotten and not needed content***. This rule does not apply to Premium members.

Pozza Ex. G (Hotfile FAQ) (emphasis added); *see also* Pozza Ex. P (Hotfile Privacy Policy) ("***All files saved by our service are deleted*** after a certain time period if you do not delete them yourself") (emphasis added). Beyond their own active deletion policies, defendants permit users to delete files at will, allowing them to protect themselves from discovery and, potentially,

liability:

> Q. Can I delete my files?
>
> A. ***Of course***. After successful uploading, you receive two links: a download link and a deletion link. Please keep both. ***If you want to remove the file from the server, you can click on the deletion link***.

Pozza Ex. G (Hotfile FAQ) (emphasis added).

Many of defendants' largest uploaders likely are criminal copyright infringers who make money by uploading popular, infringing content and, in many cases, by promoting links to that content on their own pirate websites. Uploading users brag publicly, but anonymously, on third-party link sites that they are engaged in such activities. *See* Pozza Exs. Q-S. These commercial infringers have every incentive to hide their activities from discovery in litigation as soon as they learn of a lawsuit. Case after case against end-user defendants has borne out that such infringers will act on that incentive by attempting to destroy critical evidence. *See supra* at 10-12. Yet, despite their obligation to put in place a litigation hold, defendants apparently did not change this policy ***even after they were sued*** at least twice for copyright infringement by other copyright owners.[1] Pozza Decl. ¶ 4.

Just this past weekend, internet reports surfaced that defendants were widely disabling the accounts of infringing users and those users' content files. *See* Pozza Exs. E-F. Defendants' dramatic shift in their business practices raises even greater concerns that critical evidence is not being preserved.

II. THE SERIOUS DANGER OF DESTRUCTION OF KEY EVIDENCE IN THIS CASE WARRANTS THE ENTRY OF A PRESERVATION ORDER.

The danger that defendants and their users will destroy or permit the spoliation of key

---

[1] *See Liberty Media Holdings, L.L.C. v. Hotfile.com*, No. 3:09-CV-2396-D (N.D. Tex.) (voluntarily dismissed); *Liberty Media Holdings, L.L.C. v. Hotfile Corp.* No. 11-cv-20056-AJ (S.D. Fla.); *Perfect 10, Inc v. Hotfile Corp.*, No. 3:10-cv-02031-MMA –POR (S.D. Cal.).

electronic and other evidence compels the issuance of a preservation order.

This Court has the inherent power to issue an order requiring that defendants preserve evidence, and courts have often exercised this authority on an *ex parte* basis in piracy cases to ensure that evidence of the infringement itself is preserved. *See, e.g.*, *AT&T Broadband*, 381 F.3d at 1319 (affirming *ex parte* order under district court's traditional equitable powers); *TracFone Wireless, Inc. v. King Trading, Inc.*, No. 3-08-CV-0398-B, 2008 WL 918243, at *1 (N.D. Tex. Mar. 13, 2008) (issuing *ex parte* order to preserve evidence in infringement case); *see also Capricorn Power Co., Inc. v. Siemens Westinghouse Power Corp*., 220 F.R.D. 429, 433-34 (W.D. Pa. 2004) (court has inherent authority to order evidence preserved); *Pueblo of Laguna v. United States*, 60 Fed. Cl. 133, 135 (2004) (same).

In granting such an order, a court should consider whether "(1) there is a legitimate concern for the continuing existence and maintenance of the integrity of the evidence in question absent an order preserving the evidence; (2) such concerns outweigh any harm to the defendants that may result from a preservation order; and (3) defendants will not be unduly burdened by such an order." *TracFone Wireless*, 2008 WL 918243, at *1 (granting plaintiffs' emergency *ex parte* motion to preserve evidence and for expedited discovery); *Capricorn Power*, 220 F.R.D. at 433-34; *see also AT&T Mobility LLC v. Arena Trading, Inc.*, No. 3-08-CV-0330-P, 2008 WL 624104, at *1 (N.D. Tex. Mar. 5, 2008) (finding that movant had satisfied the three-factor test and granting plaintiffs' emergency *ex parte* motion to preserve evidence). These factors are all unquestionably satisfied here.

With respect to the first factor, there is plainly a "legitimate concern" that substantial evidence will be immediately despoiled absent a Court order. Defendants' policies are unambiguous: defendants reserve the right to delete a substantial amount of electronic data that

is critical to this action. *Supra* at 12-14. Defendants' users also can delete their uploaded files, and many of the most egregious infringers are likely to do so in the course of litigation. *Supra* at 10-14. In response to other litigation, defendants did not publicly change these policies. *Supra* at 13 & n.1. Moreover, in this case, hollow promises notwithstanding, defendants continue to refuse to enter into a stipulation that could be presented to this Court, and have flatly refused to agree to preserve highly relevant categories of evidence, including: data about users' downloads of content files (including downloads by "Premium" users and Internet Protocol ("IP") addresses that would show downloads by country), all user registration information, information about payments to defendants' "Affiliate" users, communications with users, and internal communication regarding defendants' businesses. Pozza Decl. ¶ 4.[2] Defendants' evasiveness in response to requests to preserve textbook relevant evidence further underscores the clear risk of spoliation without a Court order.

"The elaborate nature of Defendants' scheme [likewise] demonstrates that Defendants will go to great lengths to conceal the details of their [illegal] scheme." *Dell*, 2007 WL 6862341, at *2. As discussed above, *supra* at 8-9, defendants actively conceal their whereabouts by using fictitious addresses and mail drop services, and operate through shell companies to shield their infringement. As this Court has recognized, *ex parte* relief to obtain evidence is appropriate when defendants "have concealed evidence by using fictitious business, personal names, and shell entities to hide their activities," *id.*, particularly when defendants use "offshore compan[ies]" and "are thus ideally placed to simply abscond offshore with their operation and their records," *id; cf. Time Warner Cable of New York City v. Freedom Electronics, Inc.*, 897 F.

[2] Defendants have denied that they "store" certain download data but it is clear, from defendants' own statements on their website, that they receive and utilize such data. *See* Foster Decl. ¶ 13. That information includes, at a minimum, the location of the downloading user and whether the downloading user is a "Premium" user. *Id*.

Supp. 1454, 1460-61 (S.D. Fla. 1995) (granting *ex parte* preliminary relief against infringer based in part on "secretive and illicit nature of this criminal enterprise").

Further, the Eleventh Circuit and this Court have recognized that *ex parte* relief to obtain evidence is appropriate when a party shows that "[the] defendant[], ***or persons involved in similar activities***, had … concealed evidence or disregarded court orders in the past," *AT&T Broadband*, 381 F.3d at 1319 (emphasis added; alterations in original). There is no doubt that prior online copyright infringers routinely engaged in such activities. *Supra* at 10-12; *see also Dell*, 2007 WL 6862341, at *2-*3 (granting *ex parte* seizure when "other prolific cybersquatters have ignored court orders[,] counterfeiters have a reputation of avoiding court orders [and] Defendants could easily destroy their electronic records and evidence in this matter"); *In re Vuitton et Fils S.A.*, 606 F.2d 1 (2d Cir. 1999) (ordering issuance of temporary restraining order in infringement case based on actions taken by counterfeiters in prior cases); *TracFone Wireless*, 2008 WL 918243, at *1 (preservation order authorized where "defendants in similar cases have 'sold or otherwise disposed of [prepaid phones]' in their possession immediately upon being served with the summons and complaint"); *Pueblo of Laguna*, 60 Fed. Cl. at 138 (party may meet burden "by demonstrating that the opposing party has lost or destroyed evidence in the past or has inadequate retention procedures in place"). As this Court has noted, that the "the vast majority of evidence of Defendants' [illegal activity] is in electronic form and subject to quick, easy, untraceable destruction" presents an "even more compelling" reason to order evidence preservation. *Dell*, 2007 WL 6862341, at *2.

Plaintiffs therefore request that the Court order the preservation of (1) all content files, (2) all content reference data, user data and activity data, including all user download records, *see* Foster Decl. ¶¶ 13-14, (3) all communications regarding the Hotfile service including records

of communications with users and website operators via any of defendants' email systems or addresses, (4) all business and marketing plans related to defendants' Hotfile-related businesses, and (5) all internal communications between and among defendants and their employees regarding defendants' Hotfile-related businesses.[3] This evidence goes to the heart of this case. The content file and download data is direct evidence of the infringement facilitated by defendants. *See A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1014 (9th Cir. 2001) (unauthorized downloading of plaintiffs' copyrighted works constituted infringement of reproduction and distribution rights); *Columbia Pictures Indus., Inc. v. Bunnell*, 245 F.R.D. 443, 451 (C.D. Cal. 2007) (similar download evidence was key to showing infringement); *Usenet*, 408 F. Supp. 2d at 440 (same); *supra* at 8.

In addition to showing direct infringement of plaintiffs' works and the use of defendants' site for infringement, the evidence of communications with and payments to users uploading high volumes of copyright-infringing content will be directly relevant in several key ways. It will demonstrate that the "commercial sense" of Hotfile hinges on infringement, and thus it will be relevant to the inducement analysis. *See Grokster*, 545 U.S. at 940. It also will be relevant to identifying key third parties for further discovery and as potential defendants. And it will be relevant to show that defendants had the requisite knowledge to be contributory infringers, *see Cable/Home*, 902 F.2d at 845-46, and that they derived a financial benefit from downloads of infringing works, *see Napster*, 239 F.3d at 1023. As the court noted in *Usenet*, the content files and user traffic data destroyed in that case, which is similar to the data that plaintiffs seek

[3] At least some user tracking data functions appear to be outsourced to third parties. Foster Decl. ¶ 15. For this reason, plaintiffs request that the preservation order extend to all data in defendants' possession, custody, or control, even if in the possession of third parties, and plaintiffs seek to serve the preservation order on third parties maintaining evidence on defendants' behalf.

preserved here, "would have been critical in showing the extent to which Defendants' service was used for the purpose of copyright infringement - a key inquiry under each of the three theories of secondary copyright infringement." 608 F. Supp. 2d at 440; *see also Bunnell*, 245 F.R.D. 443 (ordering preservation and production of critical user download data stored on the defendants' servers); Pozza Ex. T (similar order in another online infringement case).

Any burden on defendants from being ordered to preserve the electronic evidence identified above, and indeed all relevant electronic evidence, is not likely to be substantial. *See* Foster Decl. ¶¶ 8, 9. The only potential burden is that defendants will be required to store some additional data that would otherwise be deleted. But Defendants *operate a business designed to store enormous amounts of data*. *See* Pozza Ex. G.

For these reasons, the Court should enter a preservation order in the form proposed by the plaintiffs.

III. THE COURT SHOULD ORDER LIMITED EXPEDITED DISCOVERY OF CONTENT FILES AND ASSOCIATED CONTENT REFERENCE DATA.

Even with a Court order to preserve evidence, certain sub-categories of electronic data remain highly susceptible to alteration or spoliation. Accordingly, plaintiffs additionally request that the Court grant expedited discovery of the most central, vulnerable evidence in this case – the content files and associated content reference data showing downloads of those files. Experience in other cases shows that the longer defendants have the opportunity to delete evidence, the greater the danger that they will modify or delete it. *See Bunnell*, 2007 WL 4877701, at *1-*2 (evidence altered during discovery); *Usenet*, 608 F. Supp. 2d at 434, 436 (evidence destroyed "[o]n the very day [defendants] agreed to produce [it] to Plaintiffs"); Pozza Ex. U (order regarding defendants' refusal to produce evidence in defiance of a court order in

Columbia Pictures Industries v. Fung, No. CV 06-5578 (C.D. Cal. June 8, 2007)).[4]

Courts permit parties to take expedited discovery in advance of a Rule 26(f) conference upon a showing of "good cause," which "may be found where the need for expedited discovery, in consideration of the administration of justice, outweighs the prejudice to the responding party." *UMG Recordings, Inc. v. Doe*, No. C08-1038 SBA, 2008 WL 2949427, at *3 (N.D. Cal. July 30, 2008). That good cause standard is met here. The ease of modification or destruction of such electronic data justifies immediate relief to obtain the evidence. *See Dell*, 2007 WL 6862341, at *2 (emphasis added). Further, "courts have recognized" as a general matter "that good cause is frequently found in cases involving claims of infringement and unfair competition." *Semitool, Inc. v. Tokyo Electron Am., Inc.*, 208 F.R.D. 273, 276 (N.D. Cal. 2002); *see also Grooms v. Legge*, No. 09 CV 489 IEG-POR, 2009 WL 704644 (S.D. Cal. Mar. 17, 2009); *Psychopathic Records, Inc. v. Anderson*, No. Civ. 08-13407 DT, 2008 WL 4852915 (E.D. Mich. Nov. 7, 2008); *Benham Jewelry Corp. v. Aron Basha Corp.*, No. 97 Civ. 3841 (RWS), 1997 WL 639037 (S.D.N.Y. Oct. 14, 1997).

Plaintiffs therefore request that the Court authorize targeted expedited discovery, as set forth in the Proposed Order, to permit plaintiffs (a) to request a copy of data maintained by defendants that will enable plaintiffs to identify a representative sample of the content files that reside on defendants' system and have been downloaded by other users; and (b) to obtain a copy of the identified representative sample of those content files, to be specified after analyzing the produced data. *See* Foster Decl. ¶¶ 6-8 (noting that such content reference data may be used to

[4] The fact that defendants claim to be operating in multiple foreign countries while in fact operating from Florida also points to the need for quick discovery before defendants seek to transfer evidence overseas. *See, e.g., Ayyash v. Bank Al-Madina*, 233 F.R.D. 325, 327 (S.D.N.Y. 2005) (expedited discovery warranted where the "defendants are foreign individuals and corporations who have both incentive and capacity to hide their assets").

request particular content files). As noted above, this is direct evidence of the infringement facilitated by defendants that is central to the case. *Supra* at 8, 17-18. Moreover, courts routinely rely upon sampling methodologies to provide evidence of the total volume of infringement. *See Metro Goldwyn Mayer Studios, Inc. v. Grokster, Ltd.*, 454 F. Supp. 2d 966, 985 (C.D. Cal. 2006); *Columbia Pictures Indus. Inc. v. Fung*, No. CV 06-5578 SVW (JCX), 2009 WL 6355911, at *4, *8-*9 (C.D. Cal. Dec. 21, 2009); *Usenet II*, 633 F. Supp. 2d at 151-52.

There will be no prejudice by authorizing expedited discovery in this case. Defendants would be required to produce the requested evidence in any event, and producing the databases and other files containing the requested data will be relatively straightforward and can be done without imposing a substantial burden on defendants. Foster Decl. ¶¶ 8, 9. In fact, obtaining the requested data at the outset of the case will help plaintiffs more narrowly target their later discovery requests, including requests for content files, *id*. ¶ 8, which would relieve any preservation burdens as to those files. Plaintiffs have even offered to stipulate that, once the random sample of content files is produced and verified, defendants would be relieved of their burden to continue preserving those files. Pozza Decl. ¶ 5. Plaintiffs accordingly request that, as part of the requested relief to preserve evidence, the Court order the limited expedited discovery requested above and set forth in the proposed order.

CONCLUSION

For the foregoing reasons, plaintiffs respectfully request that this emergency motion be granted.

Dated: February 22, 2011

By: s/ Karen L. Stetson
Karen L. Stetson

GRAY-ROBINSON, P.A.
Karen L. Stetson (FL Bar No. 742937)
1221 Brickell Avenue
Suite 1600
Miami, FL 33131
Phone: 305-416-6880
Fax: 305-416-6887
Karen.Stetson@gray-robinson.com

MOTION PICTURE ASSOCIATION
OF AMERICA, INC.
Daniel M. Mandil (*Pro Hac Vice to be Filed*)
Karen R. Thorland (*Pro Hac Vice to be Filed*)
15301 Ventura Blvd., Building E
Sherman Oaks, CA 91403

JENNER & BLOCK LLP
Steven B. Fabrizio (*Pro Hac Vice Pending*)
Duane C. Pozza (*Pro Hac Vice Pending*)
Luke C. Platzer (*Pro Hac Vice Pending*)
1099 New York Ave., N.W., Suite 900
Washington, DC 20001
Phone: 202-639-6000
Fax: 202-639-6066

Attorneys for Plaintiffs