

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 11-20427-JORDAN

DISNEY ENTERPRISES, INC.,  
TWENTIETH CENTURY FOX FILM CORPORATION,  
UNIVERSAL CITY STUDIOS PRODUCTIONS LLLP,  
COLUMBIA PICTURES INDUSTRIES, INC., and  
WARNER BROS. ENTERTAINMENT INC.,

*Plaintiffs,*

v.

HOTFILE CORP., ANTON TITOV, and  
DOES 1-10.

*Defendants.*

\_\_\_\_\_ /

**DEFENDANTS' MEMORANDUM OF LAW IN OPPOSITION  
TO PLAINTIFFS' "EMERGENCY" MOTION FOR  
ORDER PRESERVING EVIDENCE AND EXPEDITING DISCOVERY**

**TABLE OF CONTENTS**

I. INTRODUCTION ..... 1

II. FACTUAL BACKGROUND..... 2

    A. The Parties ..... 2

        1. Hotfile..... 2

        2. Anton Titov ..... 4

        3. Plaintiffs ..... 4

    B. The Digital Millennium Copyright Act (“DMCA”) ..... 5

    C. Hotfile’s Compliance With The Safe Harbor Provisions Of The DMCA ..... 6

        1. Hotfile’s Implementation Of Digital Fingerprinting Technology To Block Copyright Infringement..... 6

        2. Copyright Holders’ Unfettered Ability To Block Content On Hotfile’s Website Through “Special Rightsholder” Accounts ..... 6

        3. Hotfile’s Recent Strengthening Of Its “Repeat Infringer” Policy ..... 7

    D. Prior Copyright Litigation Against Hotfile..... 7

    E. Hotfile’s Preservation Of All Potentially-Relevant Evidence ..... 7

    F. Plaintiffs’ Filing Of This Motion In The Absence Of Conference With Hotfile Following Implementation Of Additional Copyright Protections Which Plaintiffs Knew Had No Bearing On Hotfile’s Preservation Of Evidence..... 8

III. LEGAL ARGUMENT ..... 9

    A. Plaintiffs Have Not Carried Their Burden For Obtaining An Unilateral Preservation Order ..... 9

    B. There Is No Merit To Plaintiffs’ “Guilt-By-Association” Argument..... 10

        1. Asset Seizure Cases Have No Application Here..... 11

        2. Spoliation Cases Are Irrelevant..... 12

    C. Plaintiffs Offer Empty Justifications For This Motion ..... 13

    D. If Any Document Preservation Order Issues, It Should Be Bilateral ..... 14

    E. No Reason Exists To Expedite Discovery – Especially Since Plaintiffs Admit In Their Complaint To Scrutinizing Hotfile For “Well Over A Year,” And Since Plaintiffs Demand Unbounded Discovery Of Over 700 Servers ..... 15

IV. CONCLUSION..... 17

## I. INTRODUCTION

Despite how many times Plaintiffs repeat the unsupported allegation, this case is not about “massive copyright infringement.” Defendant Hotfile Corp. (“Hotfile”) runs a leading file-hosting service, taking advantage of improvements in internet bandwidth and data storage. Plaintiffs may feel that they are again losing a game of “catch-up” with the latest technology, Compl. ¶ 37, but the movie studios’ inability or unwillingness to keep up is hardly copyright infringement. Hotfile.com is in full compliance with the safe harbor provisions of the Digital Millennium Copyright Act that Congress created for such valuable internet service providers.<sup>1</sup> See 17 U.S.C. § 512.

Nor is there any “emergency” to justify Plaintiffs’ Motion. As Plaintiffs acknowledge in their Complaint, they have been sending (and Hotfile has been responding swiftly to) takedown notices for “*well over a year.*” Compl. ¶ 37. Plaintiffs’ screen shots of Hotfile’s website, Compl., Exs. B & C, were printed in July 2010 – 7 months ago. The “emergency” motion was filed with a 20-page memorandum, an expert declaration, and over 100 pages of (largely inadmissible) exhibits.<sup>2</sup> But it is supported by nothing but innuendo, inaccurate speculation, and unverified assertions in the Complaint. Worse, Plaintiffs’ articulated danger of spoliation – that Hotfile continues to follow its normal policy to delete unused or unwanted files – is false. See Mem. In Supp. Of Pls.’ Emergency Mot. (“Pls.’ Mem.”) at 12-13 (citing Decl. Of Duane C. Pozza In Supp. Of Pls.’ Emergency Mot. (“Pozza Decl.”), Exs. G & P. As shown in correspondence from Hotfile’s counsel attached to Plaintiffs’ motion papers, however, Hotfile has suspended all such routine deletions as part of its litigation hold promptly instituted in response to the filing of this litigation.

---

<sup>1</sup> Defendants reserve all defenses, including defenses directed to personal jurisdiction and service of process.

<sup>2</sup> Much of Plaintiffs’ “evidence” is not admissible. The declaration of Plaintiffs’ proposed expert Ian Foster consists of speculation as to what he assumes “must be.” Decl. of Ian Foster In Supp. Of Pls.’ Emergency Mot. (“Foster Decl.”) ¶¶ 5-11 (admitting that he has not performed a full analysis of Hotfile’s systems while “draw[ing] certain conclusions about the types of data that the site must necessarily be using and/or maintaining”). The declaration of Plaintiffs’ counsel Duane Pozza consists of more unverified and unsubstantiated allegations, attaching hearsay documents containing only more hearsay. See Pozza Decl. ¶¶ 6, 17-19 (copies of blogs and webpages purportedly containing postings about Hotfile); *id.* ¶ 11; *id.*, Ex. I at 7 (citing to hearsay brief referring to hearsay statement of other person about Hotfile’s Panamanian address).

Hotfile has agreed to suspend the deletion process and will leave the files deleted by users of Hotfile on the servers. . . . Hotfile agreed to suspend the deletion of files to which access has been disabled as the result of a user request or takedown notice. Hotfile also agrees to suspend any data deletion policy that would result in the deletion of an uploaded file that has been inactive or not accessed for a period of time, and will maintain such uploaded files.

Pozza Decl., Ex. C at 2, 3. The Motion is unnecessary; Hotfile has committed to preservation.

This case bears no resemblance to the cases involving *ex parte* seizures and infamous cyber-criminals. Defendants immediately engaged counsel, took measures to preserve relevant electronically-stored information, and attempted to negotiate with Plaintiffs to avoid this needless motion. But Plaintiffs' transparent motivation is to overwhelm Defendants with heavy-handed litigation tactics – in papers apparently prepared long in advance and recycled from other cases – and smear Hotfile to the Court before it can even retain lead counsel. Plaintiffs demanded a 48-hour response to this Motion despite knowing that Hotfile was in the midst of obtaining lead counsel. *See* Pozza Decl., Ex. Y (Email from Janet Munn to Steven Fabrizio (Feb. 22, 2011, 09:20 AM) (“As you know, my clients have to retain new lead counsel.”)).

In sum, Plaintiffs' Motion is much ado about nothing. It is built on hyperbole, invective, and guilt-by-association. Hotfile and Mr. Titov run a legitimate business that fully complies with (and, indeed, embraces) the United States' copyright laws and the DMCA. Ironically, the pretext used to find an “emergency” for the filing of this obviously long-planned motion – an observed increase in the termination of Hotfile accounts over the Presidents' Day weekend – was the tightening of Hotfile's repeat infringer policy. Plaintiffs should applaud this development rather than attempt to twist it into an ill-founded allegation of evidence spoliation. For the foregoing reasons, the Court should deny Plaintiffs' motion for an evidence preservation order – or at least make it bilateral – and should deny Plaintiffs' request for irrelevant “emergency” discovery.

## **II. FACTUAL BACKGROUND**

### **A. The Parties**

#### **1. Hotfile**

Hotfile is an online file-hosting service. Decl. of Anton Titov In Supp. Of Defs.' Opp'n to Pls.' Emergency Mot. (“Titov Decl.”) ¶ 5, attached as Ex. A. It is used by businesses and consumers to store and share large electronic files. *Id.* Using Hotfile's website, for example, a

company can upload voluminous files to the 700+ servers available in Dallas, obtain a unique web link (or “URL”) to those files, share that link with selected employees, and in this way permit the employees to access and download the files remotely from any internet-enabled location. *Id.* Premium users, who pay a monthly fee, can store files indefinitely, thereby obtaining backup file storage capacity. *Id.* ¶ 7. Other uses abound. Open source software developers can store and share lengthy program files with online communities. *Id.* ¶ 5. Bloggers can swiftly share information, pictures or video. *Id.* Musicians, photographers and film-makers can promote their albums, images and movies directly to potential fans and without relying upon conventional distribution or promotion (i.e., movie studios and record companies). *Id.*

Hotfile’s “Terms of Service” and “Intellectual Property and Rights Policy” published on its website explicitly prohibit copyright infringement:

***Transmission, distribution, or storage of any materials that violate laws are forbidden. This includes without restriction . . . [materials subject to] copyright laws. . . . In using the Services, you declare and guarantee that you are the author and owner of the copyrights and/or have due licenses for the represented information. . . . Hotfile reserves the right to immediately suspend or delete the account of a client, which, in the opinion of Hotfile, offends the present agreement or laws or decisions.***

***Please do not abuse the Hotfile service by using it to distribute materials to which you do not have the rights. . . . [I]f Hotfile comes to believe in good faith that content available through the Hotfile service may infringe copyrights, it will remove or disable access to the potentially infringing materials as soon as reasonably possible.***

Pozza Decl., Ex. O at 3; *id.*, Ex. X (emphasis added). When notified of files containing allegedly-copyrighted content, Hotfile promptly removes access. It even provides copyright holders, including Plaintiffs, the unfettered ability to remove access to files by directly commanding Hotfile’s servers through special rightsholder accounts. *See infra* Part II.C.2; Titov Decl. ¶¶ 11-12.

Hotfile derives revenue from “premium” subscriptions, whereby users pay up to \$9 per month for faster downloads, permanent file storage, and other benefits. Titov Decl. ¶ 7. To drive sales of premium subscriptions, Hotfile seeks to steer more visitors to its website. Hotfile encourages traffic by remunerating those who provide it – a practice commonly known amongst internet businesses as “affiliate” advertising. Thus, for every download caused by a user participating in Hotfile’s affiliate program, that user receives at least \$0.002. Pozza Decl., Ex. H.

Despite Plaintiffs' feigned incredulity arising from Hotfile's affiliate program, *see* Pls.' Mem. at 4 ("Hotfile actually pays users[!]"), the practice of paying for referrals in business is a long-standing – if not ancient – commercial practice.

Founded in 2008, Hotfile is a Panamanian corporation with its principal place of business in Sofia, Bulgaria. Titov Decl. ¶ 8. Hotfile wholly owns Hotfile Ltd., a Bulgarian limited liability company, which supports Hotfile's website operations. *Id.* Hotfile competes with the file-hosting services provided by Google® Docs, Windows Live® SkyDrive, RapidShare®, DepositFiles®, MegaUpload®, and MediaFire® – none of whom are defendants here. *Id.*

## 2. Anton Titov

A founder, technologist and minority shareholder of Hotfile – as well as the former CEO of Bulgaria's leading web-hosting company – Anton Titov is a Russian citizen who has resided in Bulgaria for the past two decades. *Id.* ¶ 2. His wife, son, mother, and brother also live in Bulgaria, where he pays taxes, possesses bank accounts, and owns a home and a car. *Id.* Mr. Titov is also founder and President of Lemuria Communications, Inc. ("Lemuria"), which was incorporated in the United States after Hotfile learned that this was necessary to obtain Internet Protocol addresses from the Latin American governing agency for servers located outside of Latin America. *Id.* ¶ 3. Mr. Titov made his first visit to the United States in October 2009 when he traveled to Florida to set up Lemuria. In a regrettable intimidation tactic, Plaintiffs named Mr. Titov as a Defendant. He was served while vacationing in Las Vegas. *Id.* ¶ 4. In a revealing contrast, although Plaintiffs allege Lemuria "provides Hotfile Corp. with critical Internet hosting services," Compl. ¶ 11, it is not named as a defendant.

## 3. Plaintiffs

Plaintiffs are five movie studios. In distinction to Hotfile's two corporate entities in Panama and Bulgaria – which Plaintiffs characterize as "offshore entities" that "operate in the shadows" – Plaintiffs deploy 71 corporate affiliates across dozens of nations from Sri Lanka to Mexico. Similarly, where Plaintiffs impugn Hotfile as a "shell corporation," Plaintiffs' corporate entities bear names like "Walt Disney Holdings (Hong Kong) Ltd." – suggesting that Plaintiffs themselves use corporations which perform little other function than holding stock. *See* Dun & Bradstreet Business Info. Rep. for Disney Enters. Inc., dated Feb. 25, 2011, attached as Ex. B.

For decades, Plaintiffs have tried unsuccessfully to exploit copyright law to suffocate new technology perceived as threatening their control over content delivery. In *Sony Corp. v.*

*Universal City Studios*, 464 U.S. 417, 421, 442, 456 (1984), the U.S. Supreme Court rejected Universal’s and Disney’s “unprecedented attempt to impose copyright liability” upon distributors of Sony’s Betamax video tape recorder. In *UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099, 1100 (C.D. Cal. 2009), the court granted summary judgment against Universal and in favor a provider of free internet-based video-sharing capability. However, Universal succeeded in bankrupting the defendant with litigation expenses, a strategy of “murder by litigation” excoriated by one leading commentator. See Nimmer on Copyright § 12B.01[C][1] (“[It] will not serve anyone’s interest if the Internet’s backbone and infrastructure are sued out of existence for involvement in purportedly aiding copyright infringement”). Four days ago, an Australian appeals court rejected the instant Plaintiffs’ claims of copyright infringement brought against another internet service provider, iiNet Ltd. See *Roadshow Films Pty v. iiNet Ltd.*, NSD179/2010, Federal Court of Australia (Sydney) (Feb. 24, 2011), portions of the Opinion are attached as Ex. C.

**B. The Digital Millennium Copyright Act (“DMCA”)**

Congress enacted the DMCA in 1998 “to facilitate the robust development and world-wide expansion of electronic commerce, communications, research, development, and education in the digital age.” S. Rep. No. 105-190, at 1-2 (1998) (quoted in *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1141-42 (N.D. Cal. 2008)). Specifically, Congress was concerned that

without clarification of their liability, service providers may hesitate to make the necessary investment in the expansion of the speed and capacity of the Internet. . . . In short, by limiting the liability of service providers, the DMCA ensures that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will continue to expand.

*Viacom Int’l Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514, 519-524 (S.D.N.Y. 2010). The DMCA provides to internet service providers “safe harbors” from any monetary liability arising from “information residing on systems or networks at the direction of users.” 17 U.S.C. § 512(c).

To qualify for protection under the DMCA’s safe harbors, service providers like Hotfile must comply with the Act’s notice-and-takedown regime. Specifically, when a copyright holder provides notice under the DMCA of an alleged infringement, the internet service provider must expeditiously take down the links identified. *Id.* § 512(c)(3)(A)-(B). “The DMCA notification

procedures place the burden of policing copyright infringement – identifying the potentially infringing material and adequately documenting infringement – squarely on the owners of the copyright.” *Perfect 10, Inc. v. CCBill, LLC*, 488 F.3d 1102, 1113 (9th Cir. 2007); *id.* (“We decline to shift [this] substantial burden from the copyright owner to the provider.”).

**C. Hotfile’s Compliance With The Safe Harbor Provisions Of The DMCA**

Hotfile is an “online service provider” within the definition in the DMCA. 17 U.S.C. § 512(k). As required, Hotfile has a designated agent with the copyright office, *id.* § 512(c)(2); Hotfile Designation of Agent, attached as Ex. A1, and has a posted repeat infringer policy. 17 U.S.C. § 512(i)(1)(A); Pozza Decl., Ex. X at 1. Hotfile responds to DMCA takedown notices within 24 hours – a response time well within the DMCA’s requirements, *see, e.g., Io Group*, 586 F. Supp. 2d at 1150 (approving responses by service provider “on the same day the notice is received (or within a few days thereafter)”), and a level of expeditiousness lauded even in Plaintiffs’ cited authorities. *See* Pozza Decl., Ex. E (“[W]hen it comes to taking down infringing files, Hotfile are one of the fastest file-hosters to do so . . .”).

1. Hotfile’s Implementation Of Digital Fingerprinting Technology To Block Copyright Infringement

Hotfile uses MD5/SHA1 digital fingerprinting technology (“hashing”) to block copyright infringement. Titov Decl. ¶ 10. For files suspected of infringement, digital fingerprints are created, the files are immediately disabled, and any file sharing the fingerprint is blocked, and cannot be uploaded again by the same user or other users, even under a different name. *Id.* ¶ 12.

2. Copyright Holders’ Unfettered Ability To Block Content On Hotfile’s Website Through “Special Rightsholder” Accounts

Hotfile permits any verified copyright owner to open a “special rightsholder” account, which permits a copyright holder to unilaterally block any file on Hotfile’s servers without any oversight by Hotfile. *Id.* ¶ 10-12. Rightsholders need merely enter a Hotfile-generated URL for a file, and it is blocked along with all copies sharing its fingerprint. *See id.* ¶ 12, Printout of Portal Allowing Special Copyright Owners to Enter URLs for Fingerprinting & Blocking, attached as Ex. A2. Plaintiff Warner Brothers actively uses its special rightsholder account with Hotfile to block content, as does DtecNet, a third-party contractor who sends takedown notices on behalf of Plaintiffs. *Id.* ¶ 11. In short, Hotfile’s copyright measures operate in a fashion similar to YouTube’s “Claim Your Content” system upheld in *Viacom*, 718 F. Supp. 2d 514.



### 3. Hotfile's Recent Strengthening Of Its "Repeat Infringer" Policy

Since its outset, Hotfile has terminated accounts of users suspected of repeated copyright infringement in a manner compliant with the DMCA. Recently, Hotfile instituted increasingly aggressive measures against repeat infringers over the President's Day weekend. *See* Pozza Dec. Ex. E ("Hotfile Goes to War Against Copyright Infringers"). Inexplicably, Plaintiffs responded with the instant Motion, insisting, without any basis (or communication with Hotfile), that Hotfile's *suspension* of accounts necessitated *deletion* of information. This is simply untrue.

#### **D. Prior Copyright Litigation Against Hotfile**

In 2009, pornographer Liberty Media Holdings sued Hotfile in Dallas for copyright infringement. *See Liberty Media Holdings, LLC v. Hotfile.com et al*, No. 3:2009-cv-02396 (N.D. Tex. filed Dec. 16, 2009). On February 10, 2010, Liberty Media dismissed the case without prejudice following the filing of motions to dismiss. It refiled in this Court last month. *See Liberty Media Holdings, LLC v. Hotfile Corp. et al*, No. 1:11-cv-20056-AJ (S.D. Fla. filed Jan. 6, 2011). In September, pornographer Perfect 10 sued Hotfile Corp. in San Diego. *See Perfect 10, Inc. v. Hotfile Corp. et al*, No. 3:2010-cv-02031 (S.D. Cal. filed Sept. 29, 2010). Despite Plaintiffs' repeated suggestion that Hotfile destroyed evidence in those cases, in fact neither plaintiff in those other cases has shown (and no court has found) that Hotfile ever failed to meet any of its document preservation responsibilities.

#### **E. Hotfile's Preservation Of All Potentially-Relevant Evidence**

Immediately upon the filing of this case, Hotfile made sure that it retained all potentially-relevant information. Titov Decl. ¶ 15. Specifically, Hotfile ensured preservation of the following information (corresponding to the categories identified in Plaintiffs' Motion):

- Content Files. As Hotfile disclosed in writing prior to this Motion, Pozza Decl., Ex. C, Hotfile is preserving all content files on its systems – even if inactive, subject to a DMCA takedown notice, or identified for deletion by users. Hotfile took on the expense of this preservation effort itself, because Plaintiffs refused to split the cost.
- Content Reference Data, User Data and Activity Data.
  - *Content Reference Data*. Hotfile is preserving content file metadata and maintains databases of the content files on its systems. Of course, the fields in the database (such as download counts) continue to change.
  - *User data*. Hotfile maintains identifying information on its users in a database, including a list of content files a user has uploaded. Hotfile is logging events of significance, such as when a user performs a task such as

changing his or her password, but not when he or she accesses the “Frequently Asked Questions” page, for example. As demanded, Hotfile is maintaining “records of payments to users for downloads of their uploaded content.” PayPal also possesses payment information, again undercutting Plaintiff’s claim that Hotfile’s information remains in imminent danger of destruction.

- *Activity Data.* In addition to IP addresses for uploaders, which Hotfile has recorded and preserved almost since its inception, Hotfile is also logging each download of a content file, including a time stamp, user IP address, number of bytes, number of seconds for the transfer, whether the user is premium or not, TCP quality information, the IP address serving the file, user ID of the downloader (if not anonymous), and upload ID. The IP addresses for users give Plaintiffs the ability to ascertain the countries of origin for Hotfile’s users using public databases. To the extent Hotfile outsources any user-tracking data functions to third parties, such as Google Analytics, Hotfile has demanded the preservation of that information in writing.
- Communications Regarding the Hotfile Service Including Records of Communications With Users and Website Operations Via Any of Defendants’ Email Systems Or Addresses. Hotfile is preserving Hotfile-related emails for its principals and all employees. Hotfile does not record its phone calls.
- Business And Marketing Plans Related To Defendants’ Hotfile-related Businesses. As previously stated in writing, Hotfile is preserving these documents..
- Internal Communications Between And Among Defendants And Their Employees Regarding Defendants’ Hotfile-Related Businesses. Hotfile is preserving all emails regarding the Hotfile business exchanged among the principals and employees.

**F. Plaintiffs’ Filing Of This Motion In The Absence Of Conference With Hotfile Following Implementation Of Additional Copyright Protections Which Plaintiffs Knew Had No Bearing On Hotfile’s Preservation Of Evidence**

At the outset of the case, Hotfile agreed in writing to preserve many of the categories of material now sought to be preserved in Plaintiffs’ Motion. Pozza Decl., Ex. C at 3 (reflecting Hotfile’s agreement to preserve content files and business and marketing plans). Hotfile then strengthened its “repeat infringer” policy before the Presidents’ Day weekend – a fact having no bearing on document preservation. Without further discussion, Plaintiffs filed their 20-page Motion with dozens of exhibits characterizing Hotfile as criminally “unscrupulous,” and demanding a response within 48 hours while knowing that Hotfile had yet to retain lead counsel.

To meet Plaintiffs’ concern with expediting discovery, Hotfile since agreed with Plaintiffs on February 27, 2011 to conduct their conference of counsel under Rule 26(f) on April 1, 2011. (An agreed order will be filed today.) While Plaintiffs do not concede the point, the early Rule 26(f) conference effectively eliminates any possible need to expedite discovery.

### III. LEGAL ARGUMENT

#### A. Plaintiffs Have Not Carried Their Burden For Obtaining An Unilateral Preservation Order

Plaintiffs have not come close to meeting their burden to demonstrate that a preservation order is warranted against Defendants. Courts apply a three-factor test in deciding whether to issue a preservation order:

1. The level of concern the court has for the continuing existence and maintenance of the integrity of evidence in the absence of a preservation order;
2. Any irreparable harm likely to result to the party seeking preservation absent an order directing preservation; and
3. The capability of the party to maintain the evidence sought to be preserved, not only as to the evidence's original form, condition or contents, but also the physical, spatial and financial burdens created by ordering evidence preservation.

*Capricorn Power Co., Inc. v. Siemens Westinghouse Power Corp.*, 220 F.R.D. 429, 435 (W.D. Pa. 2004). Such a motion must be premised on a “*specific, significant, imminent* threat of loss”; it is not enough to simply allege an “indefinite or unspecified possibility of the loss or destruction of evidence.” *Id.*

In order to meet that burden, a party generally must demonstrate that “the opposing party has lost or destroyed evidence in the past or has inadequate retention procedures in place.” *Treppel v. Biovail Corp.*, 233 F.R.D. 363, 371 (S.D.N.Y. 2006) (quoting *Pueblo of Laguna*, 60 Fed. Cl. 133, 136 (2004)). Because parties are already legally obligated to take steps to preserve relevant evidence, “a specific order from the court directing one or both parties to preserve evidence is not ordinarily required.” *U.S. ex rel. Smith v. The Boeing Co.*, No. 05-1073-WEB, 2005 WL 2105972, at \*2 (D. Kan. Aug. 31, 2005). As one court has noted, “Preservation orders are burdensome and expensive and in the absence of a clear need should not be lightly entered.” *Valdez v. Town of Brookhaven*, CV 05-4323, 2007 WL 1988792, at \*2 (E.D.N.Y. July 5, 2007).

It is not surprising, that courts routinely *deny* motions seeking preservation orders, including in copyright infringement cases. *See, e.g., Am. LegalNet, Inc. v. Davis*, 673 F. Supp. 2d 1063 (C.D. Cal. 2009) (copyright infringement action); *Capricorn Power*, 223 F.R.D. at 437-438 (“lack of the presence of a specific, imminent threat supported by the record”); *Treppel*, 233 F.R.D. at 372-373 (S.D.N.Y. 2006) (plaintiff had not demonstrated that evidence was lost or that defendant took inadequate steps to preserve evidence); *Gregg v. Local 305 IBEW*, Case No. 1:08-cv-160, 2008 WL 5171085, at \*1 (N.D. Ind. Dec. 8, 2008) (plaintiff’s “concern” that

defendants may destroy documents insufficient where there was no evidence that defendants did not intend to comply with duty to preserve evidence); *Riego v. Carroll*, Civ. No. 08-433-SLR, 2009 WL 3448850, at \*2 (D. Del. Oct. 23, 2009) (“[I]t appears that defendants have attempted to preserve relevant discovery”); *Jardin v. Datallegro, Inc.*, Case No. 08-CV-1462-IEG-RBB, 2008 WL 4104473, \* 2 (S.D. Cal. Sept. 3, 2008) (defendants “represented to the Court that they intend to meet their discovery obligations and will meet and confer with plaintiff to define the scope of the parties’ preservation obligations and protocols”); *Marin v. Evans*, No. CV-06-3090-RHW, 2007 WL 655456, at \*1, 4 (E.D. Wash. Feb. 27, 2007) (defendants took steps to prevent destruction or spoliation of evidence and plaintiffs had not established any evidence of past destruction of evidence by defendant); *Valdez*, 2007 WL 1988792, at \*3 (clear need not shown).

Here, too, Plaintiffs have failed to make the requisite showing of a “specific, significant, imminent threat” that evidence will be lost absent a preservation order. *See Capricorn Power*, 220 F.R.D. at 435. In contrast to the alarmist **rhetoric** in Plaintiffs’ Motion, the **evidence** before the Court demonstrates that Defendants timely took action to preserve relevant evidence and implement a broad litigation hold. As explained in Part II.E, Hotfile has agreed to preserve and is preserving all content files and content file metadata on its system, user data, activity data, Hotfile-related emails (both external and internal), and business and marketing plans (to the extent such plans exist). Defendants’ counsel has engaged in a meet and confer dialogue with Plaintiffs’ counsel – which Plaintiffs unilaterally cut-off with the filing of this motion – in order to further define and come to agreement on the scope of the parties’ preservation obligations. Significantly, there is not a scintilla of evidence that Defendants have ever lost or destroyed evidence in the past. Accordingly, Plaintiffs cannot establish the first two elements of the test for granting a preservation order – that there is a threat to the integrity of the evidence absent the entry of a preservation order, or that Plaintiffs will be irreparably harmed if such an order is not entered.<sup>3</sup> *See Capricorn Power*, 220 F.R.D. at 433-434. Plaintiffs’ Motion should be denied.

**B. There Is No Merit To Plaintiffs’ “Guilt-By-Association” Argument**

Having no actual evidence that Defendants have or are likely to destroy evidence, Plaintiffs resort to a “guilt-by-association” argument, which seeks to paint Hotfile as an “online

---

<sup>3</sup> Although Defendants have not focused in this Opposition on the third element, concerning the burden of preserving evidence, *see Capricorn Power*, 220 F.R.D. at 433-434, Defendants note that when they asked Plaintiffs to share in the cost of preservation, Plaintiffs refused.

piracy defendant” who “operate[s] in the shadows” and will inevitably and unrepentantly destroy evidence given any opportunity to do so. This argument is built on a tortured misapplication of two irrelevant lines of cases, the first involving the imposition of *ex parte* injunctions against counterfeiters, the second involving sanctions motions against *pro se* defendants who destroyed evidence after being sued by record companies for downloading music. Plaintiffs’ reliance on evidence of spoliation by *unrelated* parties in *unrelated* matters to try to convince the Court that Defendants *in this case* are likely to engage in spoliation lacks legal or factual support.

1. Asset Seizure Cases Have No Application Here

Plaintiffs rely on cases involving *ex parte* motions for preliminary injunctive relief to seize assets and freeze property belonging to trademark counterfeiters and other dealers in contraband. See *Dell, Inc. v. Belgiumdomains, LLC*, No. Civ. 07-22674, 2007 WL 6862341 (S.D. Fla. Nov. 21, 2007); *AT&T Broadband v. Tech Commc’ns, Inc.*, 381 F.3d 1309 (11th Cir. 2004). The motions in those cases – in direct contrast to the instant motion – were premised on specific factual showings that the defendants were likely to abscond and destroy the fruits of their criminal activity if given notice of a lawsuit and/or a request for injunctive relief. Thus, in *AT&T Broadband*, which involved claims against an individual who sold illegal cable television descramblers, the *ex parte* application was supported by affidavits from A&T security and investigative personnel establishing that the defendant was shredding documents, possessed fake drivers licenses and had \$97,000 in cash hidden under his stairway. 381 F.3d at 1312-1313.

Similarly, in *Dell*, 2007 WL 6862341, at \*2, this Court granted an order under 15 U.S.C. § 1116(d) for the seizure of goods containing counterfeit marks. The counterfeiters in that case were cybersquatters with a “documented history of covering up their tracks by simply using a new fictitious name every time they are discovered.” *Id.* Plaintiffs’ evidentiary submissions demonstrated that the defendants were “likely to abscond offshore with their operation and their records or destroy their records if they receive notice.” *Id.* at \*5. The Lanham Act allows plaintiffs to obtain injunctive relief against counterfeiters via *ex parte* application because “counterfeiters who have no substantial investment in stationary assets will often disappear or dispose of evidence if served with a notice of hearing on preliminary injunction.” *Id.* at \*3.

This case is not remotely similar, either factually or procedurally. As explained in the Factual Background section, Hotfile and Mr. Titov run a legitimate file-hosting business similar to Google® Docs and other well known websites. They are in no way analogous to the

counterfeiters or sellers of cable descramblers in *AT&T* and *Dell*. There is no evidence whatsoever that Hotfile or Mr. Titov are likely to abscond or to destroy evidence.

The *AT&T Broadband / Dell* line of cases only applies in the unique circumstance where “providing notice to the defendant would ‘render fruitless the further prosecution of the action.’”<sup>4</sup> *Id.* at \*1 (quoting *AT&T Broadband*, 381 F.3d at 1319). This is plainly not such a case. Instead of moving *ex parte* for a seizure order on filing suit, as plaintiffs did in supposedly “controlling” cases such as *AT&T Broadband* and *Dell*, Plaintiffs here waited three weeks. Defendants have not absconded since learning of the lawsuit. Rather, they implemented a broad litigation hold and met and conferred in good faith with Plaintiffs about preservation issues.

The controlling authorities – i.e., cases that *actually involved motions for preservation orders* – unequivocally require a showing that there be a “specific, significant, imminent threat” of loss of evidence if the preservation order is not imposed. *See, e.g., Capricorn Power*, 220 F.R.D. at 435. Parties meet that burden by showing that “*the opposing party*” has lost or destroyed evidence in the past or has inadequate retention procedures in place. *Treppel*, 233 F.R.D. at 371 (emphasis added). Absent evidence of such conduct *by the defendants themselves*, courts deny preservation motions as a matter of course. *See cases cited supra*, at Part III.A.

## 2. Spoliation Cases Are Irrelevant

Plaintiffs’ numerous citations to cases involving the imposition of sanctions for spoliation of evidence are beside the point.<sup>5</sup> None of these cases involve or have any relationship to Hotfile

---

<sup>4</sup> Plaintiffs’ reliance on the *Tracfone Wireless* case is, thus, similarly misplaced. That case involved an *ex parte* motion against cellular phone counterfeiters where the plaintiff’s investigator had recovered evidence that the defendants were disposing of contraband phones in a dumpster. *Tracfone Wireless, Inc. v. King Trading, Inc.*, No. 3-08-CV-0398-B, 2008 WL 918243 (N.D. Tex. March 13, 2008). Also misplaced is Plaintiffs’ citation to *Time Warner Cable of New York City v. Freedom Elecs., Inc.*, 897 F. Supp. 1454 (S.D. Fla. 1995). That case involved a motion for a preliminary injunction and to freeze the business assets of a company selling cable television descramblers in violation of the Communications Act.

<sup>5</sup> *See, e.g., Columbia Pictures, Inc. v. Bunnell*, No. 2:06-cv-01093, 2007 WL 4877701 (C.D. Cal. Dec. 13, 2007); *Arista Records, LLC v. Usenet.com, Inc.*, 633 F. Supp. 2d 124 (S.D.N.Y. 2009); *Motown Records Co., LP v. DePietro*, Civil No. 04-CV-2246, 2007 WL 576284 (E.D. Penn. Feb. 16, 2007); *Atlantic Recording Corp. v. Howell*, No. CV-06-02076, 2008 WL 4080008 (D. Az. Aug. 29, 2008); *Arista Records, L.L.C. v. Tschirhart*, 241 F.R.D. 462 (W.D. Tex. 2006); *Interscope Records v. Leadbetter*, No. C05-1149-MJP-RSL, 2007 WL 1217705 (W.D. Wash. Apr. 23, 2007); *In re Napster, Inc. Copyright Litig.*, 462 F. Supp. 2d 1060 (N.D. Cal. 2006); *Paramount Pictures Corp. v. Davis*, 234 F.R.D. 102 (E.D. Pa. 2005).

or Mr. Titov. Moreover, not a single one of these cases involves a request for a preservation order. Rather, each of the cases involves a sanctions motion made after protracted litigation in which it was revealed during discovery that the defendants – most of them *pro se* litigants who were sued by record companies for unlawfully downloading music – had lost or destroyed evidence, usually in bad faith.

Whereas Hotfile immediately implemented a broad litigation hold and has taken significant steps to preserve relevant evidence, the defendants in these spoliation cases engaged in blatant and willful destruction of evidence and, in most cases, received harsh sanctions (in some cases, terminating sanctions) for their wrongful conduct years after cases were filed.<sup>6</sup> The fact that the defendants in these other *unrelated* cases – none of which involve Hotfile or Mr. Titov – have been sanctioned for such conduct does not and cannot establish – as Plaintiffs must – that there is a “specific, significant, imminent threat of loss” of relevant evidence in this case. The conduct by other unrelated litigants is no justification here for the imposition of the unilateral preservation order that Plaintiffs seek.

### **C. Plaintiffs Offer Empty Justifications For This Motion**

Given the absence of any facts to suggest that there is a “specific, significant, imminent threat” that evidence will be lost, Plaintiffs resort to empty and illogical justifications for this Motion. For example, Plaintiffs argue that: “Most of the key evidence in this case is in

---

<sup>6</sup> See, e.g., *Bunnell*, 2007 WL 4877701, at \*8 (granting motion for terminating sanctions against defendants after nearly two years of litigation where defendants engaged in “widespread and systematic” destruction of evidence and gave false testimony to hide the destruction); *Usenet.com*, 633 F. Supp. 2d at 142 (striking affirmative defense as spoliation sanction after two years of litigation where discovery revealed that defendants had wiped hard drives, not preserved emails, and engineered witness unavailability); *Tschirhart*, 241 F.R.D. at 466 (imposing terminating sanctions against individual whose conduct showed “blatant contempt for this Court and a fundamental disregard for the judicial process” when she used software to wipe computer hard drive after receiving notice of suit); *DePietro*, 2007 WL 576284, at \*4-\*5 (discussing appropriate sanction against *pro se* defendant at summary judgment where defendant disposed of her computer and cable modem after being notified of suit); *Howell*, 2008 WL 4080008, at \*3 (granting sanctions motion after discovery and summary judgment where *pro se* defendant wiped his hard drive after receiving notice of suit); *Leadbetter*, 2007 WL 1217705, at \*8-\*9 (discussing sanctions request at summary judgment against individual who destroyed hard drive after receiving notice of suit); *In re Napster, Inc. Copyright Litig.*, 462 F. Supp. 2d 1060 (imposing sanctions on defendants after years of litigation for failure to preserve emails); *Davis*, 234 F.R.D. at 110-114 (discussing sanctions request at summary judgment against *pro se* defendant who wiped his hard drive after receiving notice of suit).

electronic form, entirely under defendants’ control, and subject to quick and easy deletion that would render it irretrievable.” Pls.’ Mem. at 2. The same is equally true of thousands—perhaps the great majority—of lawsuits currently pending in any court. And it is well established that preservation motions should *not* be granted in the ordinary course. *See Smith*, 2005 WL 2105972, at \*2; *Valdez*, 2007 WL 1988792, at \*1, 3.

Plaintiffs also rely on statements in an outdated version of Hotfile’s Terms of Service to support their unfounded claim that Hotfile is not preserving evidence. First, as Plaintiffs are aware, these are Hotfile’s “previous” Terms of Service and, thus, are no longer in effect. Second, Hotfile suspended, and did not delete this user account information. Third, as Plaintiffs have been advised, Hotfile is preserving content files.

Most curiously, Plaintiffs rely on a blog entry entitled “Hotfile Goes to War Against Copyright Infringers” to justify bringing this motion when they did – Hotfile’s upgrading over President’s Day weekend of its policy of terminating accounts of repeat infringers. Pozza Decl., Ex. E (“Hotfile, one of the rising stars on the file-hosting scene, appears to be taking a tougher stance on copyright infringement.”). The tightening of its policy in fact had no effect on preserving evidence. Hotfile is preserving content files and user data and will continue to do so.

Lastly, Plaintiffs characterize Hotfile as “unscrupulous” and “operat[ing] in the shadows” because it is run from “offshore entities” and supposedly employs a “shell company.” Pls.’ Mem. at 8. There is nothing illegal about being a Russian living in Bulgaria or incorporating in Panama. Plaintiffs’ argument rings especially hollow given that Plaintiffs themselves operate a confusing web of “offshore entities” and at least half a dozen holding companies (e.g., Walt Disney Holdings (Hong Kong) Ltd). *See Ex. B*. There is nothing sinister let alone illegal with Hotfile’s corporate structure.

**D. If Any Document Preservation Order Issues, It Should Be Bilateral**

Although Plaintiffs have failed to establish any need for an evidence preservation order, if the Court chooses to enter one, it should be bilateral. Hotfile’s contemporaneously-filed Proposed Order sets out a straightforward reciprocal order.



**E. No Reason Exists To Expedite Discovery – Especially Since Plaintiffs Admit In Their Complaint To Scrutinizing Hotfile For “Well Over A Year,” And Since Plaintiffs Demand Unbounded Discovery Of Over 700 Servers**

Parties may not ordinarily seek discovery before they confer under Rule 26(f) to formulate “a mutually agreeable [discovery] plan.” Fed. R. Civ. P. 26(d)(1), (f) & Adv. Comm. Note (1993). The Rule exists so that “discovery can be conducted most efficiently and economically.” Fed. R. Civ. P. 26(f) & Adv. Comm. Note (1993). Courts may dispense with this requirement “in some cases, such as those involving requests for a preliminary injunction.” Fed. R. Civ. P. 26(d) & Adv. Comm. Note (1993). Thus, some courts categorically refuse to expedite discovery absent a showing akin to that required for a preliminary injunction. *See Platinum Mfg. Int’l v. UniNet Imaging, Inc.*, 2008 WL 927558, at \*1 n.3 (M.D. Fla. Apr. 4, 2008) (citing authority for proposition that “expedited discovery is appropriate when a movant demonstrates (1) irreparable injury, (2) some probability of success on the merits, (3) some connection between the expedited discovery and the avoidance of the irreparable injury, and (4) some evidence that the injury that will result without the expedited discovery looms greater than the injury that the defendant will suffer if the expedited relief is granted.”). At the very least, courts require “good cause” – which cannot exist when a plaintiff’s own delay motivates its demand for expedited discovery, *Gen-Probe, Inc. v. Amoco Corp., Inc.*, 926 F. Supp. 948, 952 (S.D. Cal. 1996), or when a plaintiff seeks overly broad discovery, *Philadelphia Newspapers, Inc. v. Gannett Satellite Info. Network, Inc.*, 1998 WL 404820, at \*2 (E.D. Pa. July 15, 1998).

Here, regardless of the legal standard applied, Plaintiffs’ admission in their Complaint that they studied Hotfile’s “massive infringement” for “well over a year” eliminates any merit from Plaintiffs’ demand for **emergency** discovery. Compl. ¶ 37; *see Gidatex S.R.L. v. Campaniello Imports, Ltd.*, 13 F. Supp. 2d 417, 419 (S.D.N.Y. 1998) (applying “preliminary injunction” standard for expediting discovery and finding that four and one-half month delay defeated movant’s request); *Gen-Probe*, 926 F. Supp. at 952 (applying “good cause” standard and denying expedited discovery where movant “ha[d] only itself to blame” for need to obtain discovery within three weeks). Not one of Plaintiffs’ cited authorities supports expediting discovery following more than a year of delay.

Expedited discovery should also be denied because the content file sampling Plaintiffs seek is irrelevant and would not prove their case. In *Viacom*, the Southern District of New York, citing Second and Ninth Circuit authority, articulated why the statistical sampling approach is

not sufficient: “It furnishes at most a statistical estimate of the chance any particular posting is infringing—and that is not a “red flag” marking any particular work...[The DMCA’s] establishment of a safe harbor is clear and practical: if a service provider knows (from notice from the owner, or a “red flag”) of specific instances of infringement, the provider must promptly remove the infringing material. If not, the burden is on the owner to identify the infringement.” *Viacom*, 718 F. Supp. 2d at 524-25. Moreover, Plaintiffs’ desire to engage in “statistical sampling” does not justify expedited discovery. If Plaintiffs want to proceed with this doubtful methodology they can do so through normal discovery channels during the course of this litigation. Their request should be denied.

“[C]ourts generally deny motions for expedited discovery when the movant’s discovery requests are overly broad,” as Plaintiffs’ are here. *Philadelphia Newspapers*, 1998 WL 404820, at \*2; *Qwest Commc’ns. Int’l v. WorldQuest Networks, Inc.*, 213 F.R.D. 418, 420 (D. Colo. 2003) (denying expedited discovery where movant sought to troll through information regarding all of defendant’s prepaid cash cards for evidence of infringement). Here, Plaintiffs seek:

Any electronic data received by Hotfile servers or otherwise created or used by Defendants (including databases) containing information regarding the content files uploaded to, stored on and/or downloaded from Hotfile, including without limitation any data identifying downloads and downloaders of such content files, and any data needed to identify a representative sample of such content files . . .

Pls.’ [Proposed] Order at 3, Dkt. No. 14-2. This calls for production of over 700 servers’ worth of information – all so that Plaintiffs may troll for instances of alleged infringement. In the words of the *Qwest* court, Hotfile is “hard pressed to define the outer boundary of [Plaintiffs’] requests.” 213 F.R.D. at 420. The 700 servers in Dallas used by Hotfile are not going anywhere, and no reason exists to produce them now.<sup>7</sup> See *Am. LegalNet, Inc. v. Davis*, 673 F. Supp. 2d

---

<sup>7</sup> Ordering immediate discovery would also deprive Hotfile of the opportunity to make any jurisdictional or procedural challenges to this suit. It would require “pre-judging” Hotfile’s defenses to lack merit – the very root of the word prejudice. See *Crown Crafts, Inc. v. Aldrich*, 148 F.R.D. 151, 152 (E.D.N.C. 1993) (no expedited discovery when impending motions may dispose of action). Hotfile, after conferring with its counsel, *may* decide the best course is to establish that it operates within the DMCA’s safe harbor provisions and decline to contest jurisdiction or service – although it is a Panamanian corporation operated from Bulgaria and is appearing specially in opposition to this Motion following service of a summons on a minority shareholder vacationing in Las Vegas. The Court, however, should not be forced to decide those issues *now* by virtue of being presented with an improper motion for expedited discovery.

1063, 1069 (C.D. Cal. 2009) (denying expedited discovery directed merely to merits of claim which would be obtainable in ordinary course of discovery).

**IV. CONCLUSION**

For the foregoing reasons, the Court should deny Plaintiffs' motion for an evidence preservation order. In the alternative, the Court should enter a bilateral evidence preservation order in the form of Defendants' Proposed Order. In either case, the Court should deny Plaintiffs' demand for expedited discovery.

Dated: February 28, 2011

Respectfully submitted,

s/ J. T. Munn  
Janet T. Munn, Fla. Bar No. 501281  
Rasco Klock  
283 Catalonia Avenue, Suite 200  
Coral Gables, Fl 33134  
Telephone: 305.476.7101  
Telecopy: 305.476.7102  
Email: [jmunn@rascoklock.com](mailto:jmunn@rascoklock.com)

And

s/ Roderick M. Thompson  
Roderick M. Thompson (*pro hac vice* pending)  
[rthompson@fbm.com](mailto:rthompson@fbm.com)  
Andrew Leibnitz (*pro hac vice* pending)  
[aleibnitz@fbm.com](mailto:aleibnitz@fbm.com)  
Deepak Gupta (*pro hac vice* pending)  
[dgupta@fbm.com](mailto:dgupta@fbm.com)  
Janel Thamkul (*pro hac vice* pending)  
[jthamkul@fbm.com](mailto:jthamkul@fbm.com)  
FARELLA BRAUN + MARTEL LLP  
235 Montgomery St.  
San Francisco, CA 94104  
Telephone: 415.954.4400  
Telecopy: 415.954.4480

*Counsel for Defendants*

**CERTIFICATE OF SERVICE**

I hereby certify that on February 28, 2011, the foregoing document was served on all counsel of record or pro se parties identified below either via transmission of Notices of Electronic Filing generated by CM/ECF or in some other authorized manner for those counsel or parties who are not authorized to receive electronically Notices of Electronic Filing.

By: s/ Janet T. Munn  
Janet T. Munn

**SERVICE LIST: CASE NO. 11-CIV-20427-JORDAN**

**GRAY-ROBINSON, P.A.**

Karen L. Stetson, Fla. Bar No.: 742937  
Email: Karen.Stetson@gray-robinson.com  
1211 Brickell Avenue  
Suite 1600  
Miami, FL 33131  
Phone: 305.416.6880  
Fax: 305.416.6887

**JENNER AND BLOCK, LLP**

Steven B. Fabrizio (*Pro Hac Vice*)  
Email: sfabrizio@jenner.com  
Duane C. Pozza (*Pro Hac Vice*)  
Email: dpozza@jenner.com  
Luke C. Platzer (*Pro Hac Vice*)  
Email: lplatzer@jenner.com  
1099 New York Ave, N.W.  
Suite 900  
Washington, DC 20001  
Phone: 202.639.6000  
Fax: 202.639.6066