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.
_____/

PLAINTIFFS' REPLY MEMORANDUM IN SUPPORT OF MOTION TO COMPEL RESPONSES TO REQUESTS FOR PRODUCTION OF DOCUMENTS AND INTERROGATORIES

PUBLIC REDACTED VERSION

Through more than four weeks of active negotiations with plaintiffs, the only significant objections defendants argued were relevance and burden; defendants now abandon those objections altogether. *Platypus Wear, Inc. v. Clarke Modet & Co.*, No. 06-20976-CIV, 2007 WL 4557158, at *2-3 (S.D. Fla. Dec. 21, 2007) (objections not raised in response to motion to compel are waived). Defendants' new objections do not fare any better. As for Content Reference and User Data, defendants now rest their argument on the Stored Communications Act ("SCA"), an objection that can only be termed frivolous given that "consent" is an express exception to the SCA and defendants' users have contractually consented to disclosure of the requested information. As for Affiliate Data, plaintiffs are seeking the identities only of defendants' most highly paid Affiliates – each of whom defendants have paid [redacted] to upload or host links to infringing content. In the structure of defendants' business, these top Affiliates are defendants' key business associates. Plaintiffs are entitled to know who they are because they are likely to be some of the most important witnesses and sources of discovery in this case. As for source code, defendants all but ignore the legion of comparable cases in which courts have ordered production of and ultimately relied on source code, and analyses based on source code, as key evidence. Instead, defendants rely on a single ruling. But *Viacom* is *sui generis* in that the source code at issue there involved what is arguably one of the most valuable and guarded trade secrets in the world, the secret algorithms for the Google search engine. This case raises no such extraordinary circumstances. Finally, on revenue data, defendants fail to rebut the obvious relevance of the limited data plaintiffs are seeking.

There is nothing unusual about the discovery plaintiffs are seeking. These are the same categories of discovery routinely sought and produced in comparable cases, and heavily relied on by courts in finding comparable infringers liable.[1]

---

[1] In ten pages plaintiffs cannot untangle defendants' many misstatements and false accusations. But, to be clear, there is no corporate relationship between any plaintiff and UMG Recordings or the *Veoh* case (Opp. at 2); plaintiffs did not "ambush" defendants with this motion (*id.*), but rather filed only after extensive negotiation and after the parties had acknowledged that they had exhausted productive discussion on these issues, *see* Reply Declaration of Duane C. Pozza in Support of Motion to Compel ("Pozza Reply Decl.") ¶¶ 2-4; and, remarkably, defendants falsely attribute their colorful "murder by litigation" quote to Nimmer, Opp. at 1, who does not appear to have ever said it. Defendants already have been chastised for having "mischaracterized" a governing legal standard, Order, Dkt #59, at n.3; defendants' opposition seems to be more of the same. Plaintiffs stand ready to respond in detail to any of defendants' false accusations as the Court would like. Here, plaintiffs will stick to the issues.

ARGUMENT

I. The Requested Content Reference and User Data Should Be Produced.

Defendants' objection to producing complete Content Reference and User Data is premised on the argument that the SCA somehow prohibits the discovery. According to defendants, because the SCA prohibits disclosure of the *content files*, plaintiffs have no right to the full Content Reference and User Data and plaintiffs' "proposed statistical analysis [is] impossible." Opp. at 7. But defendants are wrong about the SCA.

The SCA is inapplicable because defendants' users contractually agree to the disclosure of this information both in Hotfile's Terms of Service and in its Privacy Policy. The SCA explicitly permits disclosure pursuant to "the lawful consent of the originator or … the subscriber in the case of [a] remote computing service." 18 U.S.C. § 2702(b)(3). In Hotfile's Terms of Service, users explicitly grant such consent:

> Hotfile reserves the right to access, review, preserve, ***and disclose*** any User Content, as it reasonably believes is necessary to do any of the following: (1) satisfy any applicable law, regulation, ***legal process*** or governmental request… Hotfile will not reproduce, distribute, display or exploit any User Content ***except*** at your direction as part of the Service, or ***as Hotfile otherwise deems necessary to comply with any legal obligation.***

Declaration of Duane C. Pozza in Support of Motion to Compel ("Pozza Decl.") Ex. B at 2-3 (emphasis added). Hotfile's Privacy Policy, to which users also contractually agree, is equally explicit:

> Hotfile cooperates with government and law enforcement officials ***and private parties*** to enforce and comply with the law. ***We may disclose Personal Information*** and any other information about you to government or law enforcement officials or ***private parties*** if, in our discretion, we believe it is necessary or appropriate for any of the following reasons: ***to respond to legal requests*** (including court orders and subpoenas) …

Pozza Ex. C at 2 (emphasis added).

Here, there is no question that defendants' users have granted any consent necessary under the SCA. *See Deering v. CenturyTel, Inc.*, No. CV-10-63-BLG-RFC, 2011 WL 1842859, at *2-3 (D. Mont. May 16, 2011) (user agreement to online privacy policy sufficient consent under the Electronic Communications Privacy Act ("ECPA"), of which the SCA is a part); *Mortensen v. Bresnan Commc'n, LLC*, NO. CV 10-13-BLG-RFC, 2010 WL 5140454, at *5-6 (D. Mont. Dec. 13, 2010) (consent under ECPA established based on online subscriber agreement and privacy notice); *see also United States v. Noriega*, 764 F. Supp. 1480, 1491 (S.D.

Fla. 1991) (inmate consented to recording of telephone call under ECPA where orientation manual, telephone sticker, and consent form disclosed that calls could be recorded); *Perkins-Carillo v. Systemax, Inc*., No. CIV. 1:03CV2836-TW, 2006 WL 1553957, at *15-16 (N.D. Ga. May 26, 2006) (consent under ECPA satisfied by agreeing to workplace policy that permitted monitoring).[2]

Defendants' SCA argument is also a red herring in that defendants argue against production of *content files*, but plaintiffs do not seek to compel production of any content files at this time. Rather, plaintiffs seek to compel production of Content Reference and User Data, neither of which includes the actual content files, and neither of which is the "contents" of a communication subject to the SCA. Defendants do not contend that the SCA prohibits disclosure of Content Reference or User Data. Nor could they. The same *Viacom* case on which defendants rely ordered production of data *about* the actual content files – *i.e.*, data comparable to the Content Reference and User Data plaintiffs seek here. *Viacom Int'l Inc. v. YouTube Inc.*, 253 F.R.D. 256, 265 (S.D.N.Y. 2008) ("the ECPA does not bar disclosure of non-content data about the private videos (e.g., the number of times each video has been viewed on YouTube.com or made accessible on a third-party website through an 'embedded' link to the video). … Plaintiffs need the requested non-content data so that they can . . . have an opportunity to obtain discovery of allegedly infringing private videos claimed to be public."); *see also, e.g., Gilday v. Dubois*, 124 F.3d 277, 296 & n.27 (1st Cir. 1997) (information about communication, including date, time and length of a call, does not constitute "contents" of communication under ECPA); *Hill v. MCI WorldCom Commc'ns, Inc.*, 120 F. Supp. 2d 1194, 1196 (S.D. Iowa 2000) (same).

With or without the actual content files, the full Content Reference and User Data is highly relevant. That data will, for example, show downloads by U.S. users, which defendants themselves argue is necessary to show actionable infringement. Opp. at 6; *see* Mot. at 12. The data also will provide metadata such as file name and size, which will identify infringed copies of plaintiffs' copyrighted works. This data would provide evidence of direct infringement. It

---

[2] Just recently defendants made a proposal to provide plaintiffs with some subset of data and content files – *i.e.*, the content files they now say would be illegal to produce. Defendants' proposal, however, was crafted to prevent plaintiffs from being able to conduct relevant statistical analyses. It was only after plaintiffs counter-proposed reasonable changes to enable such statistical analyses that defendants, after more than five weeks of negotiations, raised their SCA objection. Pozza Reply Decl. ¶ 4.

would also enable plaintiffs to conduct their statistical analyses based on file name and other metadata. While defendants would argue this evidence is not as strong without the actual content files, because file names may not accurately identify the contents of a file or may be insufficiently descriptive, it would still be admissible and highly probative evidence to be weighed by the finder of fact.

Moreover, the full Content Reference and User Data would show which URL links were publicly posted on websites and, therefore, which files had been authorized for public distribution. Reply Declaration of Ian Foster in Support of Motion to Compel ("Foster Reply Decl.") ¶ 15. The SCA does not bar production of content files made publicly available. *See Snow v. DirecTV, Inc*., 450 F.3d 1314, 1320-21 (11th Cir. 2006) ("The legislative history and the statutory structure clearly show that Congress did not intend to criminalize or create civil liability for acts of individuals who 'intercept' or 'access' communications that are otherwise readily accessible by the general public"); H.R. Rep No. 99-647, at 66 (1986) (a user who posts a message on an online system "with a reasonable basis for knowing that such communications are freely made available to the public, should be considered to have given consent to the disclosure or use of the communication"). For this reason, courts order production of publicly available content from service providers. *E.g., Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.*, No. C 07-03952 JW, 2008 WL 3200822, at *1 (N.D. Cal. Aug. 7, 2008).[3]

Plaintiffs are entitled to obtain discovery to conduct relevant data analyses that would show the extent of infringement of plaintiffs' works and the overwhelming use of Hotfile for copyright infringement. Defendants have agreed to provide much of the requested data *fields*, Opp. at 8-9, but only for a sliver of content files – which would preclude both analyses. Defendants attempt to turn the discovery process on its head by arguing that plaintiffs must first identify each of their infringed titles, using only public sources and independent investigation, and only then request data about these infringements from defendants. First, the statistical analyses would be critical regardless of how many works are in suit. Second, quantifying the extent of infringement of plaintiffs' copyrights is hardly a "fishing expedition," Opp. at 5, or unusual, where plaintiffs have already stated an infringement claim against defendants for their

[3] The out-of-circuit authority defendants cite, *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 990 (C.D. Cal. 2010), and *Viacom*, 253 F.R.D. at 264, support plaintiffs here. Both courts held that communications were protected only when the user controlled and limited access to the communications. *Crispin*, 717 F. Supp. 2d at 991; *Viacom*, 253 F.R.D. at 264-65.

operation of Hotfile. Plaintiffs seek discovery from the best source available – defendants – to show the extent of infringement. Mot. at 8-9. That is common practice in copyright cases and even defendants acknowledge the numerous precedents. Opp. at 5. Defendants do not cite a comparable copyright case, and plaintiffs are unaware of any, that denied a plaintiff the right to take discovery as to the number of plaintiff's works infringed. To the contrary, courts have ordered defendants affirmatively to turn on server logging features to capture the relevant direct infringement data, *Columbia Pictures Industries v. Bunnell*, No. CV 06-1093FMCJCX, 2007 WL 2080419, at *4, *14 (C.D. Cal, May 29, 2007), and have sanctioned defendants for refusing to produce this data, *Columbia Pictures Industries, Inc. v. Fung*, No 06-cv-05578 (C.D. Cal. Aug. 10, 2007) (Pozza Reply Ex. B). The patent cases defendants cite on this point, Opp. at 5, are inapposite. *See Samsung SDI Co. Ltd. v. Matsushita Elec. Indus. Co. Ltd.,* No. CV 05-8493, 2007 WL 4302701, at *2-3 (C.D. Cal. June 27, 2007) (denying motion to compel where special local rule for patent cases "impos[ed] a limitation on a party seeking discovery"); *Micro Motion, Inc. v. Kane Steel Co.*, 894 F.2d 1318, 1324-25 (Fed. Cir. 1990) (quashing subpoena where litigant sought information from *nonparty* competitor).

Finally, defendants' arguments about particular fields of the data are largely non-issues:

Complete URLs. Defendants object to producing the full URL because that would be a "live" link to the content file. Opp. at 9. Provided defendants do not remove the file name or unique file identifier, and provided that each truncated URL still uniquely identifies only a single file on defendants' system, plaintiffs have no objection.

User geographic records. Plaintiffs requested both IP address and user-reported location data because it is unclear when defendants began preserving IP addresses for download and upload records. However, if defendants can assure the Court that they have preserved IP addresses for all download and upload records, plaintiffs will accept just the IP addresses.

Status of files. Defendants want to produce data showing the reason for files being disabled only for files that they disabled in response to a takedown notice. Opp. at 11. Plaintiffs, however, need data showing the reason any files were disabled, not just files disabled in response to a takedown notice. First, a defendant's disabling of files for any reason (*e.g.*, porn files) is evidence of the defendant's ability to control its system, which is relevant both to vicarious infringement and any DMCA defense. *E.g.*, *Arista Records LLC v. Usenet.com Inc.*, 633 F. Supp. 2d 124, 157 (S.D.N.Y. 2009) ("*Usenet II*") (holding same). Second, to be eligible for

DMCA safe harbor, defendants are obligated to disable infringing files when they have knowledge from any source, not just from takedown notices. *See* 17 U.S.C. § 512(c)(1)(A). Plaintiffs already have discovered evidence that defendants had knowledge of specific infringing files from sources other than takedown notices (Pozza Reply Ex. I); plaintiffs must be permitted to determine whether (and why) defendants disabled the files. *Viacom* does not provide otherwise. Opp. at 11 n.10. Even under *Viacom*, which plaintiffs believe to be wrongly decided, defendants would be ineligible for DMCA safe harbor for failing to disable specific infringing files of which they have knowledge. *Viacom Int'l Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514, 528-29 (S.D.N.Y. 2010).

II. The Requested Affiliate Data Should Be Produced.

Defendants misstate plaintiffs' request for Affiliate Data. Plaintiffs are seeking identifying Affiliate information *only* for the top 500 highest paid Affiliates (uploaders or websites). Mot. at 12-13. This information is clearly relevant. Defendants have paid these top Affiliates anywhere from [redacted] to over [redacted] for uploading content to Hotfile (in the case of users) or promoting content (in the case of websites). Pozza Ex. G. By defendants' math, each Affiliate is paid an average of $0.002 for each download of a file uploaded by the Affiliate. Opp. at 11. Thus, an Affiliate defendants paid [redacted] is responsible for uploading content downloaded [redacted]; an Affiliate defendants paid [redacted] is responsible for uploading content downloaded [redacted]. These are key business associates of defendants.

These top Affiliates, who performed crucial functions for defendants, are likely to be important witnesses and sources of relevant information and discovery. Infringers in defendants' position almost always deny their knowledge and intent. It is hardly surprising that, in numerous comparable cases, third parties, including former employees and business associates, have provided the most incriminating evidence against defendants, including key documents defendants failed to produce. *E.g.*, *Usenet II*, 633 F. Supp. 2d at 133-35 (former employees provided key evidence of misconduct); *Arista Records LLC v. Lime Group LLC*, No. 06 CV 5936, -- F. Supp. 2d --, 2011 WL 1742029, at *6 (S.D.N.Y. May 2, 2011) (former president supplied key evidence); *Columbia Pictures Indus., Inc. v. Fung*, No. CV 06-5578 SVW (JCx), 2009 WL 6355911, at *9, *13 (C.D. Cal. Dec. 21, 2009) (forum moderators); *Columbia Pictures Indus., Inc. v. Bunnell*, 06-cv-01093 FMC-JCx, 2007 WL 4877701, at *4 (C.D. Cal. Dec. 13,

2007) (former administrators). Hotfile's very top Affiliates are likely to have participated in communications with defendants revealing defendants' knowledge of, and intent to foster and profit from, infringement, as well as communications concerning defendants' efforts to undermine copyright enforcement. This is true whether or not the Affiliates themselves infringed plaintiffs' works. Opp. at 12. The ability to discover the identities of such witnesses is central to the discovery process.[4]

Defendants' privacy arguments are equally baseless. Defendants have the burden of proving that a foreign privacy law applies and would preclude disclosure. *Consejo De Defensa Del Estado De La Republica De Chile v. Espirito Santo Bank*, No. 09-20613-CIV, 2010 WL 2162868, at *2 (S.D. Fla. May 26, 2010). Defendants' bare citation to two foreign statutes without discussion or argument does not satisfy that burden. In fact, the two statutes do not bar disclosure in this case, because the Affiliate Data, by defendants' affirmative choice, resides on computer servers in the United States and defendants obtained their foreign users' consent to the transfer of this data to the United States for storage. Pozza Ex. C at 1 ("The information Hotfile collects about you and your usage of the Service will be transmitted to and stored by Hotfile on servers in the United States"). Consent to transfer to another country is an explicit exception to the cited statutes. Leibnitz Ex. K at art. 26 ¶ 1(a), Ex. J at art. 36a ¶ 6.1. Once transferred to the United States, such data is no longer governed by the European laws. *See* Pozza Reply Ex. C (Wall Street Journal, March 16, 2011) (discussing that EU is now proposing but has not yet extended law to cover data residing in non-EU countries). Moreover, both statutes have "consent" and "legal claims" exceptions under which, for the reasons discussed in regard to the SCA, disclosure would be permitted even if the statutes applied. Leibnitz Ex. K at art. 26 ¶¶ 1(a), (d); Ex. J at art. 36a ¶¶ 6.1, 6.4 (similar).[5]

Finally, there is no First Amendment issue raised by disclosure of Affiliate information. Plaintiffs are seeking disclosure of the identities of individuals because they are defendants'

---

[4] Nor is it consequential whether Affiliate witnesses reside in the United States or abroad. Indeed, given defendants' claim to operate from Bulgaria, Opp. at 13, Affiliates having close relations to defendants are likely to reside abroad.

[5] Of course, even if foreign laws prohibited disclosure, which they do not, given the importance of this data to plaintiffs, this Court could still order the discovery, particularly since defendants have not even attempted to meet their burden of proving that the relevant factors weigh in favor of nondisclosure. *E.g.,* S*ociete Nationale Industrielle Aerospatiale v. U.S. District Court*, 482 U.S. 522, 544 n.29 (1987); *Espirito Santo Bank*, 2010 WL 2162868, at *2.

business associates, not because they have engaged in a speech activity. *See SaleHoo Group, Ltd. v. ABC Co.*, 722 F. Supp. 2d 1210, 1214-15 (W.D. Wash. 2010). An offline defendant could not keep the identities of its relevant business associates secret merely because they preferred to operate anonymously. It is no different online.

III. Source Code Should Be Produced.

Access to Hotfile's source code is essential so that plaintiffs can establish technical facts directly related to their core allegations. By way of example only, defendants' source code is central to proving plaintiffs' allegation that defendants have the ability to control copyright infringement on their system, and have refused to exercise that control. *See* Compl. ¶ 62; *Usenet II*, 633 F. Supp. 2d at 157; Declaration of Ian Foster in Support of Motion to Compel ("Foster Decl.") ¶¶ 9, 11. The source code is also central to showing that defendants have the ready ability to implement effective filtering technologies to mitigate infringement. Mot. at 18; Foster Decl. ¶ 11. And source code is central to proving plaintiffs' allegations that defendants have designed their system to facilitate infringement and to undermine copyright owner enforcement efforts. Compl. ¶ 61; Mot. at 18; Foster Decl. ¶¶ 9-10. Indeed, courts in other online infringement cases have relied on source code features as proof of the defendant's knowledge of and intent to foster infringement. *Lime Group*, 2011 WL 1742029, at *19-20; *Fung*, 2009 WL 6355911, at *14; *Usenet II*, 633 F. Supp. 2d at 148, 153.

The importance of source code in this case far exceeds the "relevant and necessary" standard cited by defendants. Opp. at 14. *Only* source code analysis can definitively establish many significant technical matters in this case. Foster Decl. ¶¶ 8, 13; *see* Foster Reply Decl. ¶¶ 2-14. Defendants' assertion that observation and testing of their system from the outside, without access to source code, is sufficient is simply wrong. External observation would not enable plaintiffs to discover or analyze "administrative" functions which are only available to the site operator. *See* Foster Reply Decl. ¶¶ 7-8. External testing would not allow plaintiffs to determine whether special features are available to certain classes of users, such as top Affiliates. *Id.* ¶ 5. Nor would external testing allow plaintiffs to establish how Hotfile functioned prior to the litigation, which is plainly relevant given that defendants changed their copyright practices following the filing of this action. *Id.* ¶ 6.[6] Hotfile's source code would definitively and

[6] Plaintiffs also cannot rely on depositions of hostile engineers on complex and nuanced technology issues, especially where, as here, there will be language barriers. Even with a

unambiguously establish how Hotfile's system was designed and functions, and what it can and cannot do – as a matter of scientific fact.

The authorities do not require a showing of strict necessity, just that the code will provide evidence regarding issues central to claims or defenses in the case. *E.g.*, *In re Facebook PPC Advertising Litig.*, No. C09-03043 JF (HRL), 2011 WL 1324516, at *3 (N.D. Cal. Apr. 6, 2011) (granting production of requested source code relevant to performance of a filter, noting that no other evidence would substitute for analysis of code itself); *Metavante Corp. v. Emigrant Sav. Bank*, No. 05-CV-1221, 2008 WL 4722336, at *2 (E.D. Wis. Oct. 24, 2008).

Defendants' trade secret objection – based on a single case, in which plaintiff primarily sought production of Google's search engine source code – cannot be a bar to production of such important evidence. Google's search engine source code is one of the most closely guarded and valuable trade secrets in the world. Without doubt, Google's search engine source code – the product of "over a thousand person-***years***" of work, *Viacom*, 253 F.R.D. at 259 (emphasis added) – gives it an unparalleled advantage over competitors. That situation is *sui generis*. Defendants have not submitted evidence showing Hotfile's source code is remotely comparable. *See* Opp. Ex. 2 (Titov Decl.) ¶ 8 (vaguely indicating that "Hotfile's technology optimizes the experience for Premium users while, at the same time, providing a more efficient service for all users").

Plaintiffs provide the most pertinent authorities. Mot. at 17-18. Defendants attempt to distinguish those cases by arguing that those defendants were blatant infringers whereas Hotfile is a legitimate "storage" business. Opp. at 2, 16 & n.21. But defendants here pay uploaders for heavily downloaded content, and have publicly admonished users not to use Hotfile for storage, but only for files that will be actively promoted for distribution. Pozza Reply Exs. D-E. Defendants cannot rely on claims of innocence to bar discovery that would refute those claims.

Hotfile source code is central to this case, and there is no reason why the carefully crafted security measures contained in the Protective Order entered by this Court – negotiated specifically to protect defendants' source code – are insufficient. Mot. at 17.

IV. The Requested Monthly Revenue Information Should Be Produced.

Plaintiffs have already narrowed their request for financial information to monthly revenues related to Hotfile. Defendants ignore the obvious relevance. A defendant's intent can

---

cooperative witness, testimony on such detailed technical subject matters would result in an ambiguous and incomplete record. Foster Decl. ¶ 13.

be proven by circumstantial evidence, including motive, and the amount of profit earned from infringement is highly probative of an infringer's motive. *See Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913, 940 (2005). Plaintiffs' theory here is that defendants knowingly and intentionally promote copyright infringement *to profit from it*. Plainly, someone earning $5 million a month from infringement has a far greater incentive to encourage that infringement than someone earning $500 a month.

Moreover, defendants' argument that their "flat fee" pricing immunizes them from liability is incorrect. First, whether defendants' revenue comes from advertising or subscription payments, defendants' business model depends upon attracting subscribers using the lure of popular infringing content as the "draw." Indeed, after this litigation was filed, defendants terminated some infringers and traffic to the Hotfile website appeared to plummet. Pozza Reply Exs. F-H. The monthly revenue data should demonstrate such a drop and quantify defendants' economic incentive to turn a blind eye to repeat infringers. *E.g.*, *Ellison v. Robertson*, 357 F.3d 1072, 1079 (9th Cir. 2004) (relevant evidence includes cancellation of subscription based on lack of infringing content). Second, *Grokster*'s reliance on the "commercial sense" of the infringer's business is not limited to advertising models and, since *Grokster,* courts have applied the same analysis to subscription fee models. *Usenet II*, 633 F. Supp. 2d at 156-57. Third, defendants selectively quote from the DMCA legislative history; two sentences after the passage quoted by defendants, Congress makes clear that financial benefit "would, however, include any such [flat] fees where the value of the service lies in providing access to infringing material." S. Rep. No. 105-190, at 45 (1998); H.R. Rep. 105-551(II), at 54 (1998) (same).

Finally, defendants are mistaken that disclosure of financial information is subject to a heightened "necessary" standard. Financial information need only be relevant to be disclosed. *See Bellosa v. Universal Tile Restoration, Inc.*, No. 08-60054-CIV, 2008 WL 2620735, at *4 (S.D. Fla. June 30, 2008) (ordering production of financial records without showing of necessity); *Capone v. Estate of Ison*, No. 06-80945, 2008 WL 2277507, at *4 (S.D. Fla. May 30, 2008) (same).[7]

---

[7] Defendants citation to *Empire of Carolina, Inc. v. Mackle*, 108 F.R.D. 323 (S.D. Fla. 1985)) and two out-of-circuit cases is inapposite, because the Eleventh Circuit has declined to impose a higher standard than relevance even for disclosure of confidential tax records. *See Maddow v. Proctor & Gamble Co., Inc.*, 107 F.3d 846, 853 (11th Cir. 1997); *Bellosa*, 2008 WL 2620735, at *4 (noting same).

Dated: June 24, 2011

Respectfully submitted,

By: /s/ Karen L. Stetson
Karen L. Stetson
GRAY-ROBINSON, P.A.
1221 Brickell Avenue
16th Floor
Miami, Fl 33131
Telephone: (305) 461-6880
Facsimile: (305) 461-6887

MOTION PICTURE ASSOCIATION OF AMERICA, INC.
Karen R. Thorland (*Pro Hac Vice)*
15301 Ventura Blvd.
Building E
Sherman Oaks, CA 91403
Phone: (818) 995-6600
Fax: (818) 285-4403

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

Attorneys for Plaintiffs

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 24th Day of June, 2011, I served the following documents on all counsel of record on the attached service list via the Court's CM/ECF filing system:

Plaintiffs' Reply Memorandum in Support of Motion to Compel Responses to Requests for Production of Documents and Interrogatories

I further certify that I am admitted to the United States Court for the Southern District of Florida and certify that this certificate of Service was executed on this date at Washington, D.C.

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

SERVICE LIST

Disney Enterprises, Inc., et al. v. Hotfile Corp. et al.
CASE NO. 11-CIV-20427-JORDAN

FARELLA BRAUN + MARTEL LLP
Anthony P. Schoenberg
tschoenberg@fbm.com
Roderick M. Thompson
rthompson@fbm.com
N. Andrew Leibnitz
aleibnitz@fbm.com
Deepak Gupta
dgupta@fbm.com
Janel Thamkul
jthamkul@fbm.com
235 Montgomery Street
San Francisco, CA 94104
Phone: 415-954-4400

Attorneys for Defendants Hotfile Corp. and Anton Titov

RASCO KLOCK
Janet T. Munn
jmunn@rascoklock.com
283 Catalonia Ave., Suite 200
Coral Gables, FL 33134
Phone: 305-476-7101
Fax: 305-476-7102

Attorney for Defendants Hotfile Corp. and Anton Titov

BOSTON LAW GROUP, PC
Valentin Gurvits
vgurvits@bostonlawgroup.com
825 Beacon Street, Suite 20
Newton Centre, MA 02459
Phone: 617-928-1804

Attorneys for Defendants Hotfile Corp. and Anton Titov