JENNER & BLOCK LLP
STEVEN B. FABRIZIO (*pro hac vice*)
sfabrizio@jenner.com
KATHERINE A. FALLOW (*pro hac vice*)
kfallow@jenner.com
DUANE C. POZZA (State Bar No. 225933)
dpozza@jenner.com
601 Thirteenth Street, N.W.
Suite 1200 South
Washington, DC 20005
Telephone: 202-639-6000
Facsimile: 202-639-6066
Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

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

Plaintiffs,

v.

JUSTIN BUNNELL, FORREST PARKER, WES PARKER, VALENCE MEDIA, LLC, and DOES 1-10,

Defendants.

Case No. CV 06-1093 FMC (JCx)
DISCOVERY MATTER
The Honorable Jacqueline Chooljian

PLAINTIFFS' SUPPLEMENTAL MEMORANDUM IN SUPPORT OF PLAINTIFFS' MOTION FOR AN ORDER (1) REQUIRING DEFENDANTS TO PRESERVE AND PRODUCE CERTAIN SERVER LOG DATA, AND (2) FOR EVIDENTIARY SANCTIONS

REDACTED
FILED PURSUANT TO PROTECTIVE ORDER

Date: April 3, 2007
Time: 9:30 a.m.
Ctrm: 20

Discovery Cut-off: May 4, 2007
Pretrial Conf. Date: Oct. 22, 2007
Trial Date: Dec. 4, 2007

The server data at issue *exists and is used* by defendants in responding to every user request to download a dot-torrent file. J. Stip. 9:5-11:22; 20:10-21:8; Horowitz Decl. ¶¶ 10-14. Defendants do not deny this; nor could they. Nor do defendants deny that they readily could preserve this data simply by "turning on" the logging function that comes with their server software. In the face of these uncontroverted facts, defendants' claim that they have no obligation to preserve this data is baseless. As defendants know, the server data provides critical evidence of which dot-torrent files are actually being downloaded from the TorrentSpy site, and is directly probative of central issues in this case. Try as defendants might to obfuscate the issues, defendants' so-called "privacy" and First Amendment arguments provide no justification for their destruction of important evidence.

I. Preserving the Existing User Request Data Is Necessary and Simple.

As set forth in plaintiffs' contentions and the declaration of Professor Horowitz, the user request data at issue *already exists*. The data is sent by users to the TorrentSpy server every time they request a webpage or seek to download a dot-torrent file, and defendants' server ***must*** process that data in order for users to obtain the dot-torrent file. J. Stip. 9:5-11:22; 20:10-21:8; Horowitz Decl. ¶¶ 10-14. While accusing plaintiffs of "subterfuge," J. Stip. 31:6, defendants never dispute that this is how their technology works. Indeed, it is defendants who confuse two separate issues – whether the user request data actually exists and whether the server logs currently exist. The issue is not whether the server log files exist – they apparently do not because defendants have deliberately chosen not to keep them. But defendants do not, and cannot, deny that the user request data itself *does exist*, at least until defendants erase it.

The fact that defendants must take some (minimal) affirmative steps to preserve this data does not mean that defendants are "creating new evidence." The law is clear that once a party is required to preserve existing evidence, a party must take affirmative steps to preserve it, such as moving emails that might otherwise be

automatically deleted to permanent storage. *E.g., In re Napster, Inc. Copyright Litig.*, 462 F. Supp. 2d 1060, 1070 (N.D. Cal. 2006) (party must preserve emails that would otherwise be deleted under existing retention policy); *Nat'l Ass'n of Radiation Survivors v. Turnage*, 115 F.R.D. 543, 557-58 (N.D. Cal. 1987) "The obligation to maintain discoverable materials is an affirmative one[.]"). Such preservation steps are not unusual and do not constitute "creating evidence." And as plaintiffs' expert has made clear, the logging functionality already exists on defendants' server software, and it is easily enabled.[1]

For these central reasons, this case is not at all like the cases cited by defendants, *Alexander v. FBI*, 194 F.R.D. 305 (D.D.C. 2000), and *Paramount Pictures Corp. v. ReplayTV*, No. 01-9358, 2002 WL 32151632 (C.D. Cal. May 30, 2002). In *Alexander*, the plaintiffs sought to discover a list of persons whose FBI reports had been requested by the White House during the tenure of a certain employee. *Id.* at 310. The court held that defendants were not required to produce a list because no such list existed; it would have to be created. Here, by contrast, plaintiffs are asking the Court to order defendants to preserve evidence that is *currently in existence.* This is no different than the well-established requirement that a party to litigation must take affirmative steps to preserve emails after litigation commences – even if the party had a pre-existing policy to routinely destroy emails for innocent business reasons.

The Court's order in the *ReplayTV* case is equally inapposite. That case did not involve data that already existed and was routinely sent by users ***to a central***

---

[1] Defendants misleadingly suggest that they would have to "install" a logging functionality to preserve the user request server log data. J. Stip. 34:2, 5, 7, 10. But no separate installation is required – as Professor Horowitz notes, the logging functionality is a standard feature of defendants' own web server software, IIS 6.0. Horowitz Decl. ¶¶ 9-10. The defendants merely need to turn this functionality on.

server and in fact used by those servers to respond to user requests. In other words, in contrast to the situation here, *ReplayTV* did not involve the preservation of existing data. Instead, it involved data about ReplayTV users' individual activities that the Court found "is not now and has never been in existence." 2002 WL 32151632 at *2. Indeed, in *ReplayTV*, the Court noted that to collect the data plaintiffs requested, "defendants would be required to undertake a major software development effort, incur substantial expense, and spend approximately four months doing so." *Id.* at 3. Here in contrast, the defendants need only take the minimal step of turning on the logging functionality already present in their existing software – a function that is "on" by default.

II. The Privacy and First Amendment Arguments Are Meritless.

The "privacy" concerns cited by defendants are red herrings. It is telling – though not surprising – that defendants' real privacy concerns relate to *the very users who are using TorrentSpy to infringe plaintiffs' copyrighted works*. *See* J Stip. 6:5-7 (expressing concern that server log data be used for "DMCA search warrants"); 36:2-7 (same for "subpoenas"); 38:18-19 (same). But it is specious for defendants to argue that they should not be required to log user activity because they deliberately chose to switch off their servers' default logging function in order to assure their users that their infringing activities would not be monitored.[2]

---

[2] Defendants suggest that the behavior of users on the site will change once defendants begin keeping server log data. J. Stip. 42:16-26. In other words, defendants are concerned that infringing activity may decrease if infringers are aware that logs of their downloads are being kept. That is not a legitimate argument against *preserving evidence* in this case. It also supports a finding of direct infringement as a sanction, as requested by plaintiffs, J. Stip 28:21-29:23. To the extent defendants are suggesting that they will encourage their users to alter their downloading behavior to artificially manipulate the data for purposes of this litigation, defendants should be ordered to refrain from doing so.

At bottom, users do not have an expectation of privacy in the data they voluntarily send to a third-party server, including their IP address information. *See, e.g., Smith v. Maryland*, 442 U.S. 735, 743-44, 99 S.Ct. 2577, 61 L. Ed. 220 (1979). Further, the IP address information on its face does not identify any particular individual, and it is the type of information that users should expect any interactive website to receive – and keep. *See* Horowitz Decl. ¶ 13 (noting that the normal practice is to retain user request data). And this case is wholly unlike *Gonzales v. Google, Inc.*, 234 F.R.D. 674 (N.D. Cal. 2006), where the *government* sought search term data from a third party and the court noted the "difference between a private litigant revealing potentially sensitive information and having the information be produced to the Government pursuant to civil subpoena" – namely that the government may use then use that information for a criminal prosecution. *Id.* at 687. Defendants' privacy arguments ring especially hollow given that defendants [redacted] As part of defendants' document production, [redacted] Declaration of Duane C. Pozza, dated March 20, 2007, ¶ 2, Ex. 1, 2. [redacted][3]

[3] [redacted]

(continue...)

At any rate, defendants have completely ignored plaintiffs' offer, made repeatedly, to accept on an initial basis the server log data with IP address information redacted (provided defendants preserve the IP address data). J. Stip. 3:16-18; 24:15-18. The fact that defendants do not even address this argument shows that the "privacy" arguments are nothing more than a smokescreen. Plaintiffs do not believe that this step is necessary – but as a last resort, it alleviates any of defendants' so-called privacy concerns, while assuring that evidence demonstrating the actual uses of defendants' website will be preserved. Defendants also fail to explain why the privacy concerns would not be resolved by recourse to an attorneys' eyes only designation under the protective order, as would be the normal approach. *See* J. Stip. 24:8-14 (citing cases).

Finally, no legitimate First Amendment concerns are present here. It is undisputed that copyright infringement itself is not protected speech. *See A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1028 (9th Cir. 2001). And the information plaintiffs are seeking here would not reveal the identities of individual users, only their IP addresses. In the unlikely event plaintiffs ever needed to take the additional step of seeking discovery from Internet Service Providers to learn the real world identities of users from those IP addresses, the subpoena process would provide the requisite safeguards. In the very cases cited by defendants, *see* J. Stip. 38:1-8, courts have unequivocally held that copyright plaintiffs may seek discovery of infringers' identities notwithstanding any First Amendment concerns.[4]

(continued from previous page)

[redacted] March 20, 2007 Pozza Decl. Ex. 2, 3 (emphasis added).

[4] *See,.e.g, In re Verizon Internet Servs., Inc.*, 257 F. Supp. 2d 244, 257, 260-67 (D.D.C. 2003), *rev'd on other grounds*, 351 F.3d 1229 (D.C. Cir. 2003); *Sony Music Entm't Inc. v. Does 1-40*, 326 F. Supp. 2d 556, 567-68 (S.D.N.Y. 2004).

Respectfully submitted,

Dated: March 20, 2007

JENNER & BLOCK LLP

By: _____
KATHERINE A. FALLOW

STEVEN B. FABRIZIO
KATHERINE A. FALLOW
DUANE C. POZZA
JENNER & BLOCK LLP

KAREN R. THORLAND
W. ALLAN EDMISTON
LOEB & LOEB LLP

GREGORY P. GOECKNER
LAUREN T. NGUYEN
15503 Ventura Boulevard
Encino, CA 91436

Attorneys for Plaintiffs

PROOF OF SERVICE

I, Vicki S. Henderson, the undersigned, declare that:

I am employed in the County of Los Angeles, State of California, over the age of 18, and not a party to this cause. My business address is 10100 Santa Monica Boulevard, Suite 2200, Los Angeles, California 90067-4120.

On March 20, 2007, I served a true copy of the **PLAINTIFFS' SUPPLEMENTAL MEMORANDUM AND DECLARATION OF DUANE C. POZZA IN SUPPORT OF PLAINTIFFS' MOTION FOR AN ORDER (1) REQUIRING DEFENDANTS TO PRESERVE AND PRODUCE CERTAIN SERVER LOG DATA, AND (2) FOR EVIDENTIARY SANCTIONS** on the parties in this cause by placing the above named document in a sealed envelope addressed as set forth below, or on the attached service list. I caused each such envelope, with postage thereon fully prepaid, to be deposited for collection and mailing with the United States Postal Service in accordance with Loeb & Loeb LLP's ordinary business practices.

Ira P. Rothken
ROTHKEN LAW FIRM
3 Hamilton Landing, Suite 224
Novato, CA 94949

Kirk J. Retz, Esq.
Retz & Hopkins LLP
21535 Hawthorne Boulevard, Suite 200
Torrance, CA 90503

I am readily familiar with Loeb & Loeb LLP's practice for collecting and processing correspondence for mailing with the United States Postal Service and Overnight Delivery Service. That practice includes the deposit of all correspondence with the United States Postal Service and/or Overnight Delivery Service the same day it is collected and processed.

I certify that I am employed in the office of a member of the bar of this Court at whose direction the service was made.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on March 20, 2007, at Los Angeles, California.

Vicki S. Henderson

LA1531424.1
20335110010
01/08/2007 vsh