EXHIBIT E

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

COLUMBIA PICTURES INDUSTRIES, et al.,

Plaintiffs,

v.

GARY FUNG, et al.,

Defendants.

Case No. CV 06-5578 SVW(JCx)

ORDER (1) GRANTING IN PART AND DENYING IN PART PLAINTIFFS' MOTION TO REQUIRE DEFENDANTS TO PRESERVE AND PRODUCE SERVER LOG DATA AND FOR EVIDENTIARY SANCTIONS; AND (2) GRANTING PLAINTIFFS' REQUEST FOR ATTORNEYS' FEES AND COSTS

[UNDER SEAL]

I. SUMMARY

Pending before the court is plaintiffs' motion to require defendants to preserve and produce certain electronic data, and for evidentiary sanctions and attorneys' fees, based upon defendants' alleged failure to preserve and produce all such data.

Based upon the court's consideration of the arguments and evidence presented, and the applicable law, the court finds and orders: (1) the data in issue is relevant and within the scope of information sought by plaintiffs' discovery requests; (2) the data constitutes "electronically stored information" and is or was

137

within the possession, custody and control of defendants; (3) defendants have failed to demonstrate that the preservation and production of such data is unduly burdensome, or that the other reasons they articulate justify the ongoing failure to preserve and produce such data; (4) defendants must preserve the data within their possession, custody or control and produce any such data in a manner which masks the Internet Protocol addresses ("IP addresses") of the computers used by those accessing defendants' website;[1] (5) evidentiary sanctions against defendants for spoliation of evidence are not appropriate; and (6) awarding attorneys' fees and costs are appropriate.

II. PROCEDURAL HISTORY

On September 26, 2006, plaintiffs filed a First Amended Complaint ("Complaint") against defendants for copyright infringement. Plaintiffs allege, inter alia, that defendants knowingly enable, encourage, induce, and profit from massive online piracy of plaintiffs' copyrighted works through the operation of their internet websites. The Complaint is predicated on theories of contributory infringement, secondary infringement, and inducement. Defendants filed an Answer on November 28, 2006.

On March 26, 2007, plaintiffs filed a "Joint Stipulation Regarding Plaintiffs' Motion for an Order Requiring Defendants to (1) Produce and (2) Preserve and Produce Certain Server Log Data (3) for Evidentiary Sanctions,

---

[1]An IP address is a standard way of identifying a computer that is connected to the Internet. United States v. Heckenkamp, 482 F.3d 1142, 1144 (9th Cir. 2007). With an IP address, a party could identify the Internet Service Provider ("ISP") providing internet service to the user of the computer corresponding to such IP address. See In Re Charter Communications, Inc., 393 F.3d 771, 774 (8th Cir. 2005). Only the ISP, however, could link the particular IP address to an individual subscriber. Id. As in the case of a subscriber to a particular telephone number, the identity of the subscriber to an IP address is not necessarily indicative of the person using the service at a given time.

and (4) for Attorneys' Fees and Costs" ("Plaintiffs' Motion"), a declaration of plaintiffs' counsel Gianni P. Servodidio ("Servodidio I Decl."), and a declaration of plaintiffs' expert Ellis Horowitz ("Horowitz I Decl.").[2] On the same date, defendants filed opposing declarations of defendants' counsel Ira P. Rothken ("Rothken Decl.") and Jared R. Smith ("Smith Decl."), and a declaration of defendant Gary Fung ("Fung I Decl."), as well as accompanying exhibits to each declaration.

On April 2, 2007, plaintiffs filed another declaration of Ellis Horowitz ("Horowitz II Decl."). On April 4, 2007, plaintiffs filed under seal a supplemental memorandum ("Plaintiffs' Supp. Memo I") and a declaration of plaintiffs' counsel Sami J. Valkonen ("Valkonen Decl.") with exhibits.

On April 10, 2007, the court directed the parties to file additional items. On April 17, 2007, plaintiffs filed under seal another memorandum ("Plaintiffs' Supp. Memo II") and additional declarations of Gianni P. Servodidio ("Servodidio II Decl.") and Ellis Horowitz ("Horowitz III Decl."). On the same date, defendants filed a supplemental memorandum ("Defendants' Supp. Memo"), and another declaration of Gary Fung ("Fung II Decl.").

On April 27, 2007, plaintiffs filed under seal another declaration of Gianni P. Servodidio ("Servodidio III Decl."). On May 22, 2007, defendants filed another declaration of Gary Fung ("Fung III Decl.").

Plaintiffs' Motion requests that the court issue an order requiring defendants to preserve and produce certain data responsive to plaintiffs' First Request for

///

///

---

[2]On March 27, 2007, plaintiffs filed a notice of errata regarding Plaintiffs' Motion. A corrected version of Plaintiffs' Motion was attached thereto as Exhibit 1.

Production of Documents, Request Nos. 23 and 25.[3] Specifically, plaintiffs request that defendants be ordered to preserve, to the extent not already preserved, and to produce in native format, server logs and databases of the activities of users of defendants' websites and communications between such users and defendants' websites, including: (i) the IP addresses of the users of defendants' websites who request dot-torrent files or hash-links – the functional equivalent of dot-torrent files; (ii) the specific dot-torrent files or hash-links requested by the users; (iii) the dates and times of such requests; (iv) reports from users' computers confirming that the actual download of the desired content item corresponding to the dot-torrent file or hash-link has been completed by the user; and (v) the IP addresses of users who are downloading content items and who themselves seek the IP

---

[3]Plaintiffs electronically served their First Request for Production of Documents on November 2, 2006. (Servodidio I Decl., Ex. J at 111).

Request No. 23 seeks "all documents that identify the dot-torrent files, torrents, hash-links, and releases that have been made available by, searched for, or downloaded by users of the Fung Websites and Trackers including documents that identify the users who have made available, searched for, or downloaded such dot-torrent files, torrents, hash-links, and releases." (Servodidio I Decl., Ex. D at 42).

Request No. 25 seeks "all documents, including server logs, databases of a similar nature, or reports derived from such logs or databases, that [defendants] maintain, have ever maintained, or have available that record the activities of the Fung Websites and Trackers or their users, including documents concerning . . .Electronic communications of any type between the Fung Websites and Trackers and users; . . . Logs of user activities; . . . Logs or records of dot-torrent files or torrents made available, uploaded, searched for, or downloaded on Ishohunt, Torrrentbox or Podtropolis; . . .Logs or records of hash-links or messages containing hash-links made available, searched for or otherwise obtained at Ed2k-it; and . . . Logs or records of releases documented, searched for, or reviewed on Isohunt." (Servodidio I Decl., Ex. D at 44-45).

addresses of other users who have a desired content item (collectively "Server Log Data.").[4] Plaintiffs also request that the court require defendants to pay reasonable expenses incurred in making Plaintiffs' Motion, including attorneys' fees, pursuant to Fed. R. Civ. P. 37(a)(4)(A).

On April 10, 2007, the court took Plaintiffs' Motion under submission pursuant to Rule 78 of the Federal Rules of Civil Procedure and Local Rule 7-15.[5]

III. FACTS

Defendants operate four websites (Isohunt, Torrentbox, Podtropolis, and Ed2k-it) and two trackers (one associated with TorrentBox, and one associated with Podtropolis) (collectively "Fung websites" or "defendants' websites").[6] (Horowitz I Decl. ¶ 1; Horowitz III Decl. ¶ 2).

The Fung websites offer dot-torrent files (or their functional equivalent – hash-links) for download by users.[7] (Horowitz I Decl. ¶¶ 4, 5). The dot-torrent

---

[4]Plaintiffs' Motion and many of the documents filed by both parties thereafter, speak in more general terms about the data in issue. The most clear and precise statement of the data sought by Plaintiffs' Motion is set forth in the Servodidio III Declaration, at paragraph 4.

[5]The court was simultaneously considering a motion raising similar issues in the case entitled Columbia v. Bunnell, No. 06-1093 FMC(JCx) (the "Bunnell matter"), in which the parties are represented by the same counsel involved in this action. This court held an evidentiary hearing and heard extensive arguments from the parties in connection with the similar motion in the Bunnell matter.

[6]Defendants' company, website servers, and computers are all located in Canada. (Fung I Decl. ¶ 9).

[7]Three of defendants' websites – Isohunt, Torrentbox, and Podtropolis – utilize the BitTorrent technology and offer dot-torrent files for download by users. (Horowitz I Decl. ¶ 5). The fourth website – Ed2k-it – is an analogous site which utilizes the eDonkey protocol, and offers access to hash-links which are the (continued...)

files/hash-links offered on the Fung websites do not contain actual copies of full-length content items, such as movies. (Horowitz I Decl. ¶ 6). Rather, they contain data used by a BitTorrent or eDonkey "client" application on a user's computer to access the content in issue. (Horowitz I Decl. ¶ 4).

A typical dot-torrent file contains the IP addresses of one or more computers known as "trackers." (Horowitz I Decl. ¶ 6). A "tracker" directs a user's computer where to find peers who have all or part of a particular content file by providing the user's computer with the IP addresses of those peers' computers. (Horowitz III Decl. ¶ 3). The tracker receives reports during the peer-to-peer transfer of the actual content items and receives confirmation from the user's computer once the download has been completed. (Horowitz III Decl. ¶ 3).

If a user of defendants' websites clicks on a "download torrent" or hash-link, the web server receives the user request, including the user's IP address and the name of the requested dot-torrent file or hash-link. (Horowitz I Decl. ¶ 11). Such data passes fleetingly through the random access memory ("RAM") and is written to temporary files on defendants' hard disks in the transient disk space.[8] (Fung I Decl. ¶ 3; Fung II Decl. ¶ 4). By virtue of being written to temporary files on defendants' transient disk space, such data is deleted continually and overwritten in the ordinary course of business. (Fung I Decl. ¶ 3; Fung II Decl. ¶ 4).

///

///

---

[7](...continued)
functional equivalent of dot-torrent files from a user's standpoint. (Horowitz I Decl. ¶¶ 4, 5).

[8]RAM is a form of temporary storage that every computer uses to process data. (Horowitz II Decl. ¶ 9).

Defendants do, however, appear to retain certain categories of Server Log Data in the ordinary course of their business. The court will collectively refer to the following five such categories of data as the "Currently Preserved Data."

First, some Server Log Data is stored in aggregate form without "personal identifying information"[9] through defendants' use of Google Analytics.[10] (Fung I Decl. ¶ 3).

Second, as to *registered* users of the Isohunt website only, defendants appear to store such specific users' downloading activity to enable the functioning of its Search History Manager.[11] (Horowitz I Decl. ¶ 19).

---

[9]Defendants use the term "personal identifying information" to encompass IP addresses. (Fung I Decl. ¶ 3). However, they cite to no authority for the proposition that IP addresses are properly included in this term. Even defendants' privacy policy for Isohunt, parenthetically refers to "personal information" as "email address, etc." and does not expressly include IP addresses. Nor is it clear to the court that an IP address, in and of itself, necessarily constitutes "personally identifying information." See supra note 1.

[10]Google Analytics is a service used to monitor users' views of particular web pages, including search pages for dot-torrent files. (Horowitz II Decl. ¶ 11). Google Analytics logs activity from specific web pages where the website operator has inserted a script directing the user requests to be sent to Google Analytics. (Horowitz II Decl. ¶ 12). When a user requests a page from a website, the user's computer is instructed to send information to the Google Analytics website. (Horowitz II Decl. ¶ 11). At a later time, the website operator can access information collected by Google Analytics about the website user's activities. (Horowitz II Decl. ¶ 11). Services like Google Analytics typically aggregate information and do not supply raw logs. (Horowitz II Decl. ¶ 12).

[11]The Search History Manager feature of the Isohunt website allows registered users to monitor their past downloads of torrent files from the site. (Servodidio I Decl. ¶ 8, Ex. G). Defendants have produced to plaintiffs portable document format printouts for the Search History Manager database. (Servodidio II Decl. ¶ 4). However, as of April 17, 2007, it does not appear that defendants

(continued...)

Third, as to the Isohunt website only, defendants also appear to store certain such data through their use of IPRO Corporation ("IPRO"), a third party service providing web usage statistics similar to Google Analytics.[12] (Horowitz II Decl. ¶ 13).

Fourth, with respect to the Torrentbox website and its associated tracker, defendants appear to be programmatically logging and reading from a database (i) the number of user downloads of dot-torrent files; and (ii) the number of the completed user downloads of the content item associated with the dot-torrent file. (Horowitz III Decl. ¶ 6, Ex. A).

Finally, at least as to the Torrentbox tracker, it also appears that the software used by defendants causes to be written to a database: (i) IP addresses of users making requests to the tracker's server seeking the IP addresses of other users who have the desired content item available for sharing; and (ii) reports from the user's computer confirming that the actual download of the desired content item corresponding to the dot-torrent file has been completed by the user.[13] (Horowitz III Decl. ¶¶ 4, 5).

---

[11](...continued)
have produced the Search History Manager database in its native format. (Servodidio II Decl. ¶ 2).

[12]The Isohunt website contains a script resulting in user visits being logged by IPRO. (Horowitz II Decl. ¶ 13). Each time a user's web browser visits a web page on Isohunt, the user's browser sends IPRO various information including the specific web pages visited. (Horowitz II Decl. ¶ 13). This also results in the disclosure of the user's IP address and information regarding a user's search queries to IPRO. (Horowitz II Decl. ¶ 13).

[13]Aside from preservation in the normal course of business, discussed above, defendants also affirmatively retained certain "snapshots" of their database for purposes of this litigation. (Fung I Decl. ¶ 2; Servodidio I Decl., Ex. K at 113). Defendants produced such snapshots, which did not include IP addresses, e-mail addresses or website addresses, to plaintiffs in this action. (Fung I Decl. ¶ 2).

On October 30, 2006, plaintiffs sent a written notice to defendants' counsel formally reminding counsel and defendants of their obligation to preserve all potentially discoverable evidence related to this litigation ("October Letter"). (Servodidio I Decl., Ex. J at 107-09). The October Letter specifically noted that "[o]nce a party reasonably anticipates a litigation, **it must suspend its routine document retention / destruction policy** and put in place a 'litigation hold' to ensure the preservation of relevant documents." (Servodidio I Decl., Ex. J at 107) (emphasis in original). The October Letter further specifically referred to the need to preserve electronic files, and to take steps to prevent the destruction or deletion thereof. (Servodidio I Decl., Ex. J at 107). Among other things, the October Letter expressly includes in the items to be preserved, "logs of user activity even if heretofore your clients had automatically set up their systems to discard them." (Servodidio I Decl., Ex. J at 107).[14]

IV. DISCUSSION

A. The Server Log Data Is Relevant

Pursuant to Rule 26(b)(1) of the Federal Rules of Civil Procedure, parties may obtain discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party. Fed. R. Civ. P. 26(b)(1). Plaintiffs contend that the Server Log Data is relevant to numerous claims and defenses, including whether defendants' users have directly infringed plaintiffs' copyrighted works, and the extent to which the Fung websites are used for purposes of copyright infringement. (Plaintiffs' Motion at 5, 22-26). The court agrees.

This case is predicated on theories of vicarious infringement, contributory infringement, and inducement. (Complaint ¶¶ 41-43). Primary infringement is a necessary predicate to such claims. Perfect 10, Inc. v. Amazon.com, Inc., 2007 WL 1428632, at *15 (9th Cir. May 16, 2007) (citing A&M Records, Inc. v.

---

[14]Prior to the filing of Plaintiffs' Motion, the docket does not reflect that plaintiffs sought a preservation order.

Napster, Inc., 239 F.3d 1004, 1013 n.2 (9th Cir. 2001)). Defendants contest primary infringement. (Answer ¶ 40).

There can be no serious dispute that the Server Log Data is relevant to whether the users of the Fung websites are primary infringers, and that such data may be key to the instant action.

B. The Server Log Data Constitutes Electronically Stored Information and Is Discoverable

Rule 34(a) of the Federal Rules of Civil Procedure provides for the discovery of documents or electronically stored information – including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained. Fed. R. Civ. P. 34(a). "Rule 34(a) applies to information that is fixed in a tangible form and to information that is stored in a medium from which it can be retrieved and examined." Advisory Comm. Notes to the 2006 Amendment of Rule 34. The Advisory Committee Notes further indicate that Rule 34(a)(1) "is expansive and includes any type of information that is stored electronically," and that it "is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and development." Id.

Defendants argue that the Server Log Data does not constitute electronically stored information and is not discoverable under Fed. R. Civ. P. 34(a) because such data has never been electronically stored on their websites or in any medium from which the data can be retrieved or examined, or fixed in any tangible form. (Plaintiffs' Motion at 39-41; Defendants' Supp. Memo at 1-2; Fung I Decl. ¶ 3). More specifically, defendants contend that since such data is transient and would require the installation of equipment for its storage, it cannot constitute electronically stored information. (Defendants' Supp. Memo at 1-2). Plaintiffs assert that such data is electronically stored information because it is being logged

and written on the hard drives of defendants' servers where it is copied and stored. (Plaintiffs' Supp. Memo I at 2; Horowitz II Decl. ¶¶ 3-5).

First, as to the Currently Preserved Data, there is no question that such data is stored in a medium from which defendants can retrieve and examine it, and thus that it constitutes electronically stored information in defendants' possession, custody or control.

Second, as to the remaining Server Log Data, such data, at a minimum, passes through RAM and is written to temporary files on hard disks of the Fung websites. (Fung II Decl. ¶¶ 3, 4). Although the parties have presented no authority which deals with whether data that passes through RAM and is written only to temporary files in transient space constitutes "electronically stored information" under Rule 34, defendants do rely upon a case in which the Ninth Circuit addressed whether data in RAM – a medium more transient than temporary files on a hard drive – is electronically stored information in another context. (Valkonen Decl., Ex. B at 2). In MAI Sys. Corp. v. Peak Computer Inc., 991 F.2d 511, 518-19 (9th Cir. 1993), the Ninth Circuit determined in the context of the Copyright Act, that software copied into RAM was "fixed" in a tangible medium and was sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration.[15] It

---

[15]The Ninth Circuit effectively reaffirmed the continuing viability of MAI in its recent opinion Perfect 10, Inc. v. Amazon.com, Inc., 2007 WL 1428632 (9th Cir. May 16, 2007). In that case, the court stated: "A photographic image is a work that is '"fixed" in a tangible medium of expression' for purposes of the Copyright Act, when embodied (i.e., stored) in a computer's server (or hard disk, or other storage device). The image stored in the computer is the 'copy' of the work for purposes of copyright law. See MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 517-18 (9th Cir. 1993) (a computer makes a 'copy' of a software program when it transfers the program from a third party's computer (or other storage device) into its own memory, because the copy of the program recorded in

(continued...)

defined RAM as "a computer component in which data and computer programs can be temporarily recorded." Id. at 519 (citing Apple Computer, Inc. v. Formula International, Inc., 594 F. Supp. 617, 622 (C.D. Cal. 1984) (describing the copying of programs into RAM as a "temporary fixation")). RAM has elsewhere been described as providing "temporary storage." See Adobe Systems Inc. v. Macromedia, Inc., 201 F. Supp. 2d 309, 318 (D. Del. 2002) (characterizing RAM as "temporary storage"); see also Apple Computer, Inc. v. Franklin Computer Corp., 714 F.2d 1240, 1243 n.3 (3d Cir. 1983) ("RAM...is a chip on which volatile internal memory is stored which is erased when the computer's power is turned off.").

Other courts have concluded that even deleted data on a hard drive which can be overwritten – similar to the temporary files in issue here – are discoverable under Rule 34, without addressing whether such data constitutes "electronically stored information." See, e.g., Simon Property Group L.P. v. mySimon, Inc., 194 F.R.D. 639, 640 (S.D. Ind. 2000) (computer records, including records that have been deleted are documents discoverable under Rule 34); Playboy Enterprises, Inc. v. Welles, 60 F. Supp. 2d 1050, 1053 (S.D. Cal. 1999) (granting plaintiff access to defendant's computer hard drive so that plaintiff could attempt to retrieve deleted e-mails therefrom); Antioch Co. v. Scrapbook Borders, Inc., 210 F.R.D. 645, 652 (D. Minn. 2002) ("[i]t is a well accepted proposition that deleted computer files, whether they be e-mails or otherwise, are discoverable."); Balboa Threadworks, Inc. v. Stucky, 2006 WL 763668, at *4 (D. Kan. 2006) (granting access to hard drive of computer which may contain electronic data responsive to document request). At least one court has also found that data erased from hard drives in the

---

[15](...continued)
the computer is 'fixed' in a manner that is 'sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration.'" Perfect 10, Inc., 2007 WL 1428632, at *6.

normal course of business does not render such data undiscoverable, and that the use of an external storage media may be necessary to preserve it. See In re Cheyenne Software, Inc., 1997 WL 714891, at *2 (E.D.N.Y. 1997) (awarding monetary sanctions based on defendants' destruction of data on computer hard drives in the ordinary course of business, and noting that such data could have been copied to other storage media).

In light of the Ninth Circuit's decision in MAI, and the similarity between the definitions of electronically stored information in the Advisory Committee Notes to Rule 34 and the Copyright Act, the latter of which was in issue in MAI, this court concludes that data in RAM constitutes electronically stored information under Rule 34. Since data in RAM is more transient in nature than data in temporary files on a hard drive in transient space, and in light of the authorities referenced above, the court likewise concludes that data in temporary files on hard disks constitutes electronically stored information under Rule 34. As the Server Log Data in issue is, at a minimum, temporarily stored on defendants' hard drives in transient space, the court finds that such data constitutes electronically stored information within defendants' possession, custody or control which is discoverable under Rule 34.

C. Requiring the Preservation and Production of the Server Log Data Is Not Tantamount to Requiring the Creation of New Data

Rule 34 only requires a party to produce documents that are already in existence. Alexander v. FBI, 194 F.R.D. 305, 310 (D.D.C. 2000). Accordingly, "a party cannot be compelled to create, or cause to be created, new documents solely for their production." Paramount Pictures Corp. v. Replay TV ("Replay TV"), 2002 WL 32151632, at *2 (C.D. Cal. 2002) (citing Alexander, 194 F.R.D. at 310).

Defendants argue that because their websites allegedly have never recorded or stored the Server Log Data, requiring defendants to retain such data would be tantamount to requiring them to create a record for production in discovery.

(Plaintiffs' Motion at 38-44; Fung I Decl. ¶ 3). Plaintiffs contend that such data already exists because it is written, copied and stored on the hard drives of defendants' servers, subject to the affirmative decision by defendants as to when such data will be discarded or written over. (Plaintiffs' Supp. Memo I at 2; Plaintiffs' Supp. Memo II at 2-3; Horowitz II Decl. ¶ 5).

First, as to the Currently Preserved Data, there again is no question that such data currently exists and that the production thereof would not require the creation of new data solely for production in discovery.

Second, as to the remaining Server Log Data, the court concludes, as suggested by its analysis above, that such data exists and is, at a minimum, temporarily stored on defendants' hard drives.

As the Server Log Data exists, and is in defendants' possession, custody or control, defendants would not be required to create new information to produce it. This case is thus distinguishable from Replay TV, 2002 WL 32151632 (C.D. Cal. 2002) and Alexander, 194 F.R.D. 305 (D.D.C. 2000) on which defendants heavily rely. In both of those cases, the courts found that the information sought by plaintiffs was never in existence. See Replay TV, 2002 WL 32151632, at *2 (C.D. Cal. 2002) (denying production of customer data because such information "is not now and has never been in existence"); Alexander, 194 F.R.D. at 310 (denying production of certain list of names because there was no evidence that list existed and that the responding party was in possession of such list). In the instant case, because the Server Log Data already exists, is temporarily stored on hard drives, and is controlled by defendants, an order requiring defendants to preserve and produce such data is not tantamount to ordering the creation of new data.

///

///

///

D. An Order Requiring the Preservation of the Server Log Data Is Appropriate

Plaintiffs' Motion requests that the court issue an order requiring defendants to preserve the Server Log Data, to the extent such data is not already preserved. Plaintiffs contend, inter alia, that defendants are and have been obligated to preserve the Server Log Data, and that copying and storing such data to an external hard drive at minimal expense and effort would impose no undue burden or cost on defendants. (Plaintiffs' Supp. Memo II at 10; Horowitz II Decl. ¶ 6). Defendants object to plaintiffs' request for a preservation order on the grounds that the Server Log Data is not subject to any preservation obligation and such preservation would be unduly burdensome. (Plaintiffs' Motion at 60-62; Fung II Decl. ¶ 4).

In determining whether to issue a preservation order, courts undertake to balance at least three factors: (1) the level of concern the court has for the continuing existence and maintenance of the integrity of the evidence in the absence of an order directing preservation; (2) any irreparable harm likely to result to the party seeking the preservation of the evidence 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. v. Siemens Westinghouse Power Corp., 220 F.R.D. 429, 432-33 (W.D. Pa. 2004).

As defendants do not currently retain and affirmatively object to retention of certain Server Log Data, and in light of the key relevance of such data in this action, the first two factors clearly weigh in favor of requiring preservation of such data.

///

The third factor requires more analysis. As the "burden" issues relative to preservation significantly overlap with the "burden" issues relative to production, the court will address such issues together.

1. Technical Issues

Defendants represent that their servers do not have the capacity to record, store or copy the Server Log Data on an ongoing basis, and that the retention of such data would negatively affect the functionality of their websites, and would appear to require the installation and servicing of new equipment. (Fung II Decl. ¶ 4). However, defendants' assessment regarding the burden of recording, storing or copying the data is speculative and lacks foundation as defendant Fung represents that he has not inquired as to whether such an installation is possible or necessary, or investigated the methods and costs thereof. (Fung II Decl. ¶ 4).

Plaintiffs contend that recording, storing and copying the Server Log Data would be a trivial matter and that defendants could simply copy the data to a storage media, such as a DVD or an external hard drive. (Horowitz II Decl. ¶ 6). Plaintiffs assert that the addition of such an external hard drive to a server would place minimal additional demands on the system, and would be extremely unlikely to affect the system's performance. (Horowitz II Decl. ¶ 6). Plaintiffs further contend, based largely on statistics provided by defendants, that a one terabyte hard drive costing approximately $500 would easily facilitate storing a month's server logs for the Fung websites. (Horowitz II Decl. ¶ 7).

Based upon the evidence presented, the court finds that defendants have failed to demonstrate that they would suffer an undue technical burden as a consequence of retaining and producing the Server Log Data.

///

///

///

2. Privacy/First Amendment/Federal Statutory Issues

Defendants also raise issues concerning the privacy of their website users based upon the First Amendment and a federal statute.[16] (Plaintiffs' Motion at 47-55; Defendants' Supp. Memo at 2-4). Although the court discusses each such issue below, the court does not find defendants' arguments to be persuasive, particularly in light of the fact that this order directs defendants to mask users' IP addresses before the Server Log Data is produced. The court finds that defendants' asserted interest in maintaining the privacy of the users of their websites can be adequately protected by the protective order already entered in this action and the masking of the users' IP addresses. See A. Farber & Partners, Inc. v. Garber ("Farber"), 234 F.R.D. 186, 191 (C.D. Cal. 2006).

(a) First Amendment

Defendants contend that the First Amendment protects anonymous speech on the internet, and that the preservation and production of IP addresses – a component of the Server Log Data in issue – would encroach upon the Fung website users' First Amendment rights.

The First Amendment does protect anonymous speech, at least in circumstances involving core First Amendment expression such as political

---

[16]Defendants argue that an order requiring defendants to preserve and produce the Server Log Data would be "antagonistic" to their privacy policy. (Plaintiffs' Motion at 46). Defendants have not satisfied the court that this is actually the case. First, only one of the Fung websites – Isohunt – even appears to have a privacy policy. (Servodidio II Decl. ¶ 5; Fung I Decl. ¶ 5, Ex. A). Second, it is not at all clear that the Isohunt privacy policy applies to IP addresses. The policy advises users that the site will not "disclose [the user's] personal information (email address, etc.) or activity on this website to any third party, without the user's permission." (Fung I Decl., Ex. A). The term "personal information" is not defined. The policy does not mention IP addresses. As discussed in note 1, supra, an IP address does not itself identify a particular user of a website.

speech. See McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995) (discussing central role of anonymous speech in free marketplace of ideas). At least one court, in the context of a third party subpoena, has also concluded that the anonymous use of file sharing/copying networks to download and disseminate copyrighted material without permission qualifies for minimal First Amendment protection subject to other considerations. In re Verizon Internet Services, Inc., 257 F. Supp. 2d 244, 260 (D.D.C.), rev'd on other grounds, 351 F.3d 1229 (D.D.C. 2003).

This court assumes, without deciding that the users of defendants' websites are entitled to limited First Amendment protection. However, even assuming such protection applies, the court finds that the preservation and disclosure of the Server Log Data does not encroach or substantially encroach upon such protection, particularly in light of the fact that such data does not identify the users of defendants' websites and that the IP addresses of such users have been ordered to be masked.

(b) The Stored Communications Act[17]

Defendants appear to argue that Plaintiffs' Motion should be denied because the Stored Communications Act (18 U.S.C. §§ 2701-11) prohibits the disclosure of the Server Log Data. (Plaintiffs' Motion at 48; Defendants' Supp. Memo at 2-4). Title 18, United States Code, Section 2702, generally prohibits a person or entity providing an electronic communication service to the public from knowingly divulging the contents of a communication while in electronic storage. 18 U.S.C. § 2702(a). Specifically excepted from this prohibition are disclosures of the contents of communications (1) to an intended recipient of such communication or

---

[17]The Stored Communications Act is part of the Electronic Communications Privacy Act.

an agent thereof; or (2) with the lawful consent of an intended recipient of such communication. 18 U.S.C. §§ 2702(b)(1), 2702(b)(3).

These exceptions reflect that senders of electronic communications have no reasonable expectation that the recipients thereof will keep such communications private. Thus, when an intended recipient of electronic communications is a party to a litigation, it is that recipient's privacy which is potentially in issue. The court concludes that defendants' privacy interest in the Server Log Data is outweighed by plaintiffs' need for such data. Consequently, as defendants have the ability to consent to the disclosure of the Server Log Data, the Stored Communications Act does not provide a basis to withhold such data which is clearly within defendants' possession, custody and control.[18]

3. Impact on Good Will

Defendants also argue that they may lose good will of customers as result of the stigma that would flow from any order directing them to preserve and produce the Server Log Data. (Plaintiffs' Motion at 46-47; Fung I Decl. ¶ 6). The only evidence offered by defendants in support of this assertion is defendant Fung's declaration regarding his beliefs, with no explanation of the basis therefor. (Fung I Decl. ¶ 6).

Defendant Fung's statements regarding good will are largely speculative, conclusory, and without foundation. Nonetheless, in light of the discussion in Gonzales v. Google, Inc., 234 F.R.D. 674, 684 (N.D. Cal. 2006), the court recognizes that the preservation and production of the Server Log Data may negatively impact the way in which defendants' websites are perceived by their users and result in a loss of good will if such users are aware that such

---

[18]The good faith reliance on a court order provides a complete defense to any civil or criminal action predicated on a violation of the non-disclosure provisions of the Stored Communications Act. 18 U.S.C. § 2707(e).

preservation and production are required. Notably, these concerns did not prevent the court in Gonzales from ordering a third party to disclose certain data to the United States government.

In this case involving the preservation and disclosure by a party to another private civil litigant, the court finds that the preservation and production of the Server Log Data is appropriate in light of the conclusory and speculative nature of the evidence presented regarding the loss of good will, the key relevance and unique nature of the Server Log Data in this action, the lack of a reasonable alternative means to obtain such data, and the limitation imposed by the court regarding the masking of IP addresses.[19]

4. International Issues

Defendants further assert that any changes to the existing web servers would need to be in compliance with Canadian law because defendants are residents of Canada, the corporate entity is Canadian, and the servers are located in Canada. (Plaintiffs' Motion at 62; Fung I Decl. ¶ 9). The court is not persuaded that such concerns should relieve defendants of their obligation to preserve and produce the Server Log Data.

First, it is not clear that the Canadian legal provisions in issue apply to IP addresses, let alone to the other Server Log Data in issue. A party relying on

---

[19]Defendants suggest that Digital Millennium Copyright Act ("DMCA") subpoenas are available to plaintiffs pursuant to 17 U.S.C. § 512(h), and provide a more convenient, less burdensome, and less expensive means of obtaining the Server Log Data. (Plaintiffs' Motion at 57-60). The court rejects defendants' assertion. The DMCA permits, under circumstances specified therein, subpoenas to be issued for "information sufficient to identify [an] alleged infringer." 17 U.S.C. § 512(h)(1). Defendants have not satisfied the court that the Server Log Data (and all facets thereof) may permissibly be sought pursuant to such subpoenas, or that DMCA subpoenas are a viable alternative in this action. In any event, the court does not find that DMCA subpoenas would be "more convenient, less burdensome, or less expensive."

foreign law has the burden of showing that such law bars the discovery in issue. United States v. Vetco, 691 F.2d 1281, 1289 (9th Cir. 1981). Defendants have not met this burden.[20]

Second, even if the Canadian statutes referenced by defendants apply and are read to prohibit defendants' production of the data in issue, it is well settled that foreign blocking statutes do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute. Richmark Corp. v. Timber Falling Consultants, 959 F.2d 1468, 1474 (9th Cir. 1992) (citation and internal quotations omitted). In considering whether to excuse noncompliance with discovery orders based on foreign statutory bars, as opposed to issuance of an order directing the preservation or production of evidence which is the issue here, courts are to balance the relevant factors in issue. Id. at 1474-75. These factors include the importance of the information requested in the litigation, the degree of specificity of the request, whether the information originated in the United States, the availability of alternative means of securing the information, the extent to which noncompliance would undermine important interests of the United States or compliance would undermine important interests of the state where the information is located, and the degree of hardship on the producing party and whether such hardship is self-imposed. Richmark Corp., 959 F.2d at 1475-77. The court has weighed such factors in assessing whether to direct defendants to preserve and produce the Server Log Data – to the extent evidence bearing upon such factors has been presented. The court primarily relies upon the key relevance

---

[20]Although defendants refer to and rely upon provisions of Canadian law, they did not supply the court with copies of such provisions. (Plaintiffs' Motion at 62-63). Plaintiffs did, however, provide the court with two of the Canadian laws referenced by defendants. (Servodidio II Decl. ¶ 9, Ex. C).

of the Server Log Data to this action and the lack of alternative means to acquire such information.

In sum, defendants have failed to demonstrate that their expressed international concerns should relieve them of the obligation to preserve and produce the Server Log Data.

E. An Order Requiring the Production of the Server Log Data Is Appropriate

Defendants contend that they should not be ordered to produce the Server Log Data for the same reasons, discussed above, that cause defendants to believe that a preservation order should not issue. Plaintiffs maintain that such data should be produced, at least in a form that masks the IP addresses.

On a motion to compel discovery, the party from whom electronically stored information is sought must show that the information is not reasonably accessible because of undue burden or cost. Fed. R. Civ. P. 26(b)(2)(B). If such a showing is made, a court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Fed. R. Civ. P. 26(b)(2)(C). A court may limit discovery of electronic materials under Fed. R. Civ. P. 26(b)(2)(C) if: (i) the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues. Fed. R. Civ. P. 26(b)(2)(C).

Based on the discussion, analysis, and findings above, the court further finds: (1) defendants have failed to demonstrate that the Server Log Data is not

reasonably accessible because of undue burden or cost; (2) plaintiffs have shown good cause to order discovery of such data; (3) the discovery sought is not unreasonably cumulative or duplicative or obtainable from some other source that is more convenient, less burdensome, or less expensive; (4) plaintiffs have not otherwise had the opportunity to obtain the data sought; and (5) the burden and expense of the proposed discovery does not outweigh its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues.

F. Evidentiary Sanctions

Plaintiffs' Motion also requests evidentiary sanctions against defendants in light of defendants' alleged wilful failure to preserve, and intentional spoliation of, the Server Log Data. (Plaintiffs' Motion at 34-37).

Pursuant to Fed. R. Civ. P. 37(f), absent exceptional circumstances, a court may not impose sanctions under the discovery rules based on a party's failure to provide electronically stored information lost as a result of the routine, good faith operation of an electronic information system. Fed. R. Civ. P. 37(a). A "good faith" operation may require a party to modify or suspend certain features of that routine operation to prevent the loss of information, if that information is subject to a preservation obligation. Advisory Comm. Notes to the 2006 Amendment to Rule 37.

A litigant is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, and/or the subject of a pending discovery request. Wm. T. Thompson Co. v. General Nutrition Corp., 593 F. Supp. 1443, 1455 (C.D. Cal. 1984). Therefore, "[o]nce a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the

preservation of relevant documents." Zubulake v. USB Warburg LLC, 220 F.R.D. 212, 218 (S.D.N.Y. 2003). As a general rule, the litigation hold does not apply to inaccessible electronically stored information, such as back-up tapes, which may continue to be recycled on the schedule set forth in the company's policy. Id.

As noted above, although this court now finds that defendants have an obligation to preserve the Server Log Data that is only temporarily stored on defendants' hard drives in transient space, in the absence of (1) prior controlling precedent directly on point; and (2) a violation of a preservation order, this court finds that defendants' failure to retain the Server Log Data was based on a good faith belief that preservation of such data stored only in temporary files on their hard drives was not legally required. Consequently, the court finds that evidentiary sanctions against defendants for spoliation of evidence are not appropriate.

G. Attorneys' Fees and Costs

Plaintiffs also request that the court require defendants to pay reasonable expenses incurred in making Plaintiffs' Motion, including attorneys' fees, pursuant to Fed. R. Civ. P. 37(a)(4)(A). Plaintiffs' request for attorneys' fees and costs is granted. Defendants' failure (i) to produce, (ii) to produce in native format, and (iii) timely to produce the Currently Preserved Documents (even in a redacted form), is sufficient to cause the court to believe that attorneys' fees and costs are warranted.

V. CONCLUSION

Based upon the court's consideration of the arguments and evidence presented in conjunction with Plaintiffs' Motion, IT IS HEREBY ORDERED:

1. Defendants are directed to commence preservation of the Server Log Data to the extent not already being preserved within seven (7) days of this order and to preserve the Server Log Data for the duration of this litigation or until further order of this court or the assigned District Judge. As there may well be

multiple methods by which defendants can preserve such data, the court does not by this order mandate the particular method by which defendants are to preserve the Server Log Data.[21]

2. Defendants shall initially produce in native format the Server Log Data (with the exception noted below) by no later than two weeks from the date of this order. Defendants thereafter have a continuing obligation regularly (no less frequently than every two weeks) to update such production.[22] Although defendants are required to preserve the IP addresses encompassed within the Server Log Data, defendants are not, at least at this juncture, ordered to produce such IP addresses in an unmasked/unencrypted form. Instead, defendants shall mask, encrypt, or redact IP addresses through a hashing program or other means, provided, however, that if a given IP address appears more than once, such IP address is concealed in a manner which permits one to discern that the same IP address appears on multiple occasions.[23] Plaintiffs are prohibited from using any

---

[21]For example, if defendants are able to preserve and produce all of the Server Log Data through Google Analytics, nothing in this order precludes defendants from satisfying their obligations under this order in that fashion.

[22]The court has not limited its order to sampling at this juncture because of concerns that sampling will not provide a sufficiently representative sample of activity in light of defendants' expressed concerns regarding its notification and disclosure obligations vis-a-vis their websites' users. However, the court encourages the parties to meet and confer regarding sampling, and, if appropriate, to prepare a stipulation accordingly modifying the scope of preservation and production required by this order. In the absence of such a stipulation, the instant order is without prejudice to a request by defendants to share or shift the costs of preservation and production.

[23]For example, if, hypothetically, an IP address of "1234.5678.9101" which requested a dot-torrent file on day one at noon, was masked as "abcd.efgh.ijkl," and the same IP address requested a dot-torrent file on day two at noon,

(continued...)

means to pierce or reverse any such mask/encryption/redaction. The court does not by this order either mandate or prohibit notification to the users of defendants' websites of the fact that the Server Log Data is being preserved and has been ordered produced with masked/encrypted/redacted IP addresses.[24]

3. Plaintiffs' request for evidentiary sanctions is denied.

4. Plaintiffs' request for reasonable expenses and attorneys' fees incurred in connection with Plaintiffs' Motion pursuant to Fed. R. Civ. P. 37(a)(4)(A) is granted. Plaintiffs are directed to file a declaration setting forth the exact hours worked by counsel in connection with making Plaintiffs' Motion, the usual hourly fees of such counsel, and proof of any costs incurred by no later than **June 22, 2007**. Defendants may file an opposition challenging the reasonableness

///

---

[23](...continued)
defendants' production should reflect that "abcd.efgh.ijkl" made the request on day two at noon as well as on day one at noon.

[24]Having said that, absent further order of this court or the assigned District Judge, the Clerk is directed to file and maintain this order under seal for a period of seven (7) days. The court finds good cause to file such order under seal for at least the limited seven-day period in light of the nature of its contents and the fact that it is based, at least in part on materials submitted under seal pursuant to a protective order. The parties shall have five (5) days from the date of this order to submit any objections to the public filing of this order or any portion thereof. Any such objections should state the legal reason therefor and be accompanied by a proposed redacted version of the order which, in the objecting parties' view, is appropriate for public filing. If no objections are timely received, and absent further order of this court or the assigned District Judge, the court will direct the Clerk to file this order in the public record at the expiration of the seven-day period. Nothing in this order precludes the parties from requesting that the court unseal this order on an earlier date. The parties are further advised that this court is not inclined to stay the instant order, in light of the impending scheduling deadlines in this action and the assigned District Judge's expressed preference for matters to proceed expeditiously.

of the hours or hourly rates and costs, **by July 9, 2007**. The matter of the amount of fees and costs to be ordered will then be deemed submitted and, pursuant to Local Rule 7-15, decided without further oral argument.

IT IS SO ORDERED.

DATED: June 8, 2007

Honorable Jacqueline Chooljian
UNITED STATES MAGISTRATE JUDGE