

Only the Westlaw citation is currently available.
United States District Court, C.D. California.
COLUMBIA PICTURES INDUSTRIES, et al.,
Plaintiff,
v.
Justin BUNNELL, et al., Defendants.
No. CV 06-1093FMCJCX.

May 29, 2007.

[Duane Charles Pozza](#), [Katherine A. Fallow](#), [Steven B. Fabrizio](#), Jenner and Block, Washington, DC, [Gianni P. Servodidio](#), Jenner and Block, New York, NY, Gregory Paul Goeckner, Lauren T. Nguyen, Encino, CA, [Karen R. Thorland](#), [Walter Allan Edmiston](#), Loeb and Loeb, Los Angeles, CA, for Plaintiff.

[Ira P. Rothken](#), [Jared Robinson Smith](#), [Robert L. Kovsky](#), Rothken Law Firm, Novato, CA, [Kirk J. Retz](#), Retz and Hopkins, Torrance, CA, [Duane Charles Pozza](#), [Katherine A. Fallow](#), [Steven B. Fabrizio](#), Jenner and Block, Washington, DC, Gregory Paul Goeckner, Encino, CA, for Defendants.

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) DENYING DEFENDANTS' REQUEST FOR ATTORNEYS' FEES AND COSTS

[CHOOIJIAN](#), Magistrate J.

[UNDER SEAL]

I. SUMMARY

*1 Pending before the court are (1) plaintiffs' motion to require defendants to preserve and produce certain electronic data, and for evidentiary sanctions, based upon defendants' failure to date to preserve and produce such data; and (2) defendants' request for attorneys' fees and costs.

Based upon the court's consideration of the extensive arguments and evidence presented, the court's

assessment of the credibility of the declarants and witnesses who testified at the evidentiary hearing in this matter, and the applicable law, the court finds: (1) the data in issue is extremely relevant and within the scope of information sought by plaintiffs' discovery requests; (2) the data in issue which was formerly temporarily stored in defendants' website's random access memory ("RAM") constituted "electronically stored information" and was within the possession, custody and control of defendants; (3) the data in issue which is currently routed to a third party entity under contract to defendants and received in said entity's RAM, constitutes "electronically stored information," and is within defendants' possession, custody or control by virtue of defendants' ability to manipulate at will how the data in issue is routed; ^{FN1} (4) 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; (5) defendants must preserve the pertinent 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; (6) sanctions against defendants for spoliation of evidence are not appropriate in light of the lack of precedent for requiring the retention of data in RAM, the lack of a preservation request specifically directed to data present only in RAM, and the fact that defendants' failure to retain such data did not violate any preservation order; and (7) awarding attorneys' fees and costs are not appropriate.

^{FN1}. It may also be the case that the data in issue is within defendants' possession, custody and control by virtue of defendants' contractual relationship with the third party entity. In that circumstance, defendants would, at a minimum, have an obligation to make reasonable inquiry of the third party entity for the data in issue. See [A. Farber and Partners, Inc. v. Garber](#), 234 F.R.D. 186, 189 (C.D.Cal.2006).

II. PROCEDURAL HISTORY

On February 23, 2006, plaintiffs filed a 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 website. The complaint is predicated on theories of contributory infringement, secondary infringement, and inducement. Defendants filed an Answer on May 24, 2006.

On March 12, 2007, plaintiffs filed a "Notice of Motion and Local Rule 37-1 Joint Stipulation Regarding Plaintiffs' Motion for an Order (1) Requiring Defendants to Preserve and Produce Certain Server Log Data, and (2) for Evidentiary Sanctions" ("Plaintiffs' Motion"), a declaration of plaintiffs' counsel Duane C. Pozza ("Pozza I Decl."), a declaration of plaintiffs' expert Ellis Horowitz ("Horowitz I Decl."), a declaration of defendants' counsel Ira P. Rothken, and a declaration of defendant Wes Parker ("Parker I Decl."), as well as accompanying exhibits to each declaration. Plaintiffs' Motion requests that the court issue an order requiring defendants to preserve and produce certain data responsive to plaintiffs' First Request for Production of Documents, Request Nos. 10 and 12.^{FN2} Specifically, plaintiffs seek the preservation and production of the following data: (a) the IP addresses of users of defendants' website who request "dot-torrent" files; (b) the requests for "dot-torrent files"; and (c) the dates and times of such requests (collectively "Server Log Data").^{FN3} Plaintiffs' Motion also seeks evidentiary sanctions against defendants for their alleged spoliation of the Server Log Data. Defendants request that the court require plaintiffs to pay reasonable expenses incurred in opposing Plaintiffs' Motion, including attorneys' fees, pursuant to [F.R. Civ. P. 37\(a\)\(4\)\(B\)](#).

^{FN2}. Request No. 10 seeks "all documents that identify the dot-torrent files that have been made available by, searched for, or downloaded by users of TorrentSpy, including documents that identify the users who have made available, searched for, or downloaded such dot-torrent files." Request No. 12 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 TorrentSpy or its users, including documents concerning ... Electronic communications of any type between TorrentSpy and [users]; ... Logs of user activities; and ... Logs or records of dot-torrent files made available, uploaded, searched for, or downloaded on TorrentSpy."

^{FN3}. As the Server Log Data is temporarily stored in RAM and constitutes a document that identifies dot-torrent files that have, at a minimum, been searched for by users of TorrentSpy, it is encompassed by Document Request No. 10. Similarly, as the Server Log Data constitutes an available document concerning electronic communications between TorrentSpy and users and a record of dot-torrent files made available or searched for on TorrentSpy, it is also encompassed by Document Request No. 12.

*2 On March 20, 2007, plaintiffs filed a supplemental memorandum in support of Plaintiffs' Motion ("Plaintiffs' Supp. Memo I"), a supplemental declaration of Duane C. Pozza, and accompanying exhibits. On the same date, defendants filed a supplemental memorandum in opposition to Plaintiffs' Motion ("Defendants' Supp. Memo I") and a supplemental declaration of Wes Parker ("Parker II Decl.").

On March 21, 2007, the court directed the parties to file additional items. On March 27, 2007, plaintiffs filed a supplemental brief ("Plaintiffs' Supp. Memo II") and another declaration of Ellis Horowitz ("Horowitz II Decl."), and defendants filed a supplemental brief ("Defendants' Supp. Memo II"), a joint declaration of Justin Bunnell and Wes Parker ("Jt. Bunnell/Parker Decl."), and accompanying exhibits. On March 30, 2007, in response to the court's request that the parties submit statements as to whether certain declarants should attend and be available to testify at the hearing on this matter, the parties each submitted brief additional filings.

On April 3, 2007, the court held an evidentiary hearing at which declarants Ellis Horowitz, Wesley Parker, and Justin Bunnell testified, and the court heard the arguments of counsel.^{FN4} The court took

Plaintiffs' Motion under submission at the conclusion of the hearing.^{FN5}

^{FN4}. "RT" refers to the Reporter's Transcript of the April 3, 2007 hearing.

^{FN5}. Subsequent to the hearing, plaintiffs and defendants submitted proposed findings regarding Plaintiffs' Motion for the court's consideration.

III. FACTS^{FN6}

^{FN6}. The court finds plaintiffs' expert Ellis Horowitz to be the most credible of the three technical declarants/witnesses (*i.e.*, Horowitz, Parker, and Bunnell). To the extent the testimony and statements of Parker and Bunnell conflict with those of Horowitz, the court accepts the testimony and statements of Horowitz. The court finds that defendant Parker's testimony is credible in part and gives it some weight. However, as discussed below, the court finds that portions of Parker's declarations and testimony are unsupported and not credible. The court finds that defendant Bunnell's testimony is largely unsupported and lacks credibility.

Defendants operate a website known as "TorrentSpy" which offers dottorrent files for download by users. (Horowitz I Decl. ¶ 5). The dot-torrent files offered on defendants' website do not contain actual copies of a full-length content item. (Horowitz I Decl. ¶ 6). Rather, they contain data used by a "BitTorrent client" on a user's computer to access the content in issue. (Horowitz I Decl. ¶ 6).

As certain aspects of the technical operation of the website are relevant to the resolution of this matter, the court first sets forth its understanding and findings, based upon the evidence presented, of the operation of the relevant aspects of: (i) websites in general; (ii) defendants' website prior to the filing of Plaintiffs' Motion; and (iii) defendants' website proximate or subsequent to the filing of Plaintiffs' Motion, as the record reflects that the method of operation changed during the pendency of this action.

A. Operation of Websites in General

In general, when a user clicks on a link to a page or a file on a website, the website's web server program receives from the user a request for the page or the file. (Horowitz I Decl. ¶ 11; Horowitz II Decl. ¶ 3). The request includes the IP address of the user's computer, and the name of the requested page or file, among other things.^{FN7}(Horowitz I Decl. ¶ 11; Horowitz II Decl. ¶ 3). Such information is copied into and stored in RAM. (Horowitz II Decl. ¶ 4). RAM is a form of temporary storage that every computer uses to process data. (Horowitz II Decl. ¶ 4). Every user request for a page or file is stored by the web server program in RAM in this fashion. (Horowitz II Decl. ¶ 4). The web server interprets and processes that data, while it is stored in RAM, in order to respond to user requests. (Horowitz II Decl. ¶ 4). The web server then satisfies the request by sending the requested file to the user. (Horowitz II Decl. ¶ 3). If the website's logging function is enabled, the web server copies the request into a log file, as well as the fact that the requested file was delivered. (Horowitz I Decl. ¶ 12; Horowitz II Decl. ¶ 3). If the logging function is not enabled, the request is not retained. (Horowitz I Decl. ¶ 12; Horowitz II Decl. ¶ 3). While logging such information can be useful to a website operator in many respects, and may be a usual practice of many website operators, such logging is not essential to the functionality of a website.^{FN8} (Horowitz I Decl. ¶ 13; RT 41-42).

^{FN7}. 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.

^{FN8}. As a general matter, logging data can be useful for maintenance and upkeep of a

site, to identify and correct technical problems with the site, to examine the website traffic patterns and evaluate the performance of the site, and to audit and evaluate data related to advertising on the site. (Horowitz I Decl. ¶ 3).

B. Operation of Defendants' Website Prior to the Filing of Plaintiffs' Motion

*3 Defendants' web server is located in the Netherlands. (Jt. Bunnell/Parker Decl. ¶ 6). A factor in the decision to use a server in the Netherlands was to attract business from those individuals who did not wish their identities to be known, as defendants believe the Netherlands to have stricter privacy laws governing such information. (RT 122-23). Defendants use the web server Microsoft Internet Information Services (IIS) 6.0 to operate their website. (Horowitz I Decl. ¶ 9 Horowitz II Decl. ¶ 2; Jt. Bunnell/Parker Decl. ¶ 5). The IIS web server program contains logging functionality—meaning that it has the capacity, if the logging function is not disabled, to retain the Server Log Data. (Horowitz I Decl. ¶ 10; Horowitz II Decl. ¶ 2; Jt. Bunnell/Parker Decl. ¶ 5).^{FN9}

^{FN9}. It is the default when IIS is installed, for logging to be on. (RT 144; Horowitz I Decl. ¶ 10).

Since its inception, defendants' website's logging function has not been enabled to retain the Server Log Data. (RT 99; Parker I Decl. ¶ 3). Such logging is not necessary to, or part of defendants' business operations. (Parker I Decl. ¶ 3). The decision not to enable the logging function was based, at least in part, on the belief that the failure to log such information would make the site more attractive to users who did not want their identities known for whatever reason.^{FN10}(RT 122). Although defendants did not affirmatively retain the Server Log Data through logging or other means, the data went through and was temporarily stored in the RAM of defendants' website server for approximately six hours. (RT 47-48, 49-50, 54-55, 76; Jt. Bunnell/Parker Decl. ¶ 5).

^{FN10}. Defendants' privacy policy, which is posted on defendants' website, advises users, *inter alia*, that the site “will not collect any

personal information about you [the user] except when you [the user] specifically and knowingly provide such information.”(Parker I Decl., Ex. B). The policy further reflects that the site reserves the right at any time to modify, alter or update the policy, but that if the site does so, it will post the changes so that users are always aware of what information the site collects, how the information is used, and under what circumstances the information is disclosed. (Parker I Decl., Ex. B). Defendants have presented no evidence as to whether or how the term “personal information” is defined in the privacy policy. As an IP address identifies a computer, rather than a specific user of a computer, it is not clear that IP addresses, let alone the other components of the Server Log Data in issue, are encompassed by the term “personal information” in defendants' website's privacy policy. *See supra* note 7.

C. Operation of Defendants' Website Proximate or Subsequent to the Filing of Plaintiffs' Motion

At some point proximate or subsequent to the filing of Plaintiffs' Motion, defendants altered the method through which the website operates. (RT 54). Defendants' server no longer receives all, or all facets of the Server Log Data, or at least not in the same way.^{FN11}(RT 47, 56, 111). Instead, defendants now contract with a third party entity, “Panther,” which essentially serves as a middleman in the process. (RT 98). Panther has multiple servers around the world, including approximately 25 servers in the United States. (RT 48, 55). Requests from users who visit defendants' website for a dot-torrent file on defendants' server are now routed from a location not hosted on defendants' server to a Panther server geographically proximate to the users making the requests. (RT 53, 56-57). Panther's servers in the United States serve United States users. (RT 124). In cases involving an initial request for a specific dot-torrent file, defendants' website now receives such request from Panther. (RT 57). Defendants' website sends the requested dot-torrent file to Panther. (RT 57). Panther then sends the file to the original requesting party. (RT 57). However, once a particular dot-torrent file has been requested from defendants' website by Panther, Panther then caches it and can

provide it in response to subsequent requests for the same dot-torrent file without the need to obtain it from defendants' server. (RT 51-53, 57-58). In the latter circumstance, defendants' server no longer receives data reflecting a request to download the particular dot-torrent file. (RT 58). Thus, Panther now receives the Server Log Data in issue in its RAM. (RT 98). Panther, however, does not retain logs of such information.^{FN12}(RT 75). Defendant Parker testified that defendants switched to Panther because it allows for significantly faster processing and delivery of content. (RT 102-03). Defendants deny that the decision to contract with Panther was motivated by a desire to avoid being in possession of Server Log Data or to bypass a possible court order. (RT 50, 103, 123).^{FN13}

^{FN11}. Prior to the filing of Plaintiffs' Motion, defendants' website provided links to third-party sites that have torrent files on their sites, as well as links to torrent files on the cache of defendants' website. (RT 111). Once defendants made the recent change in their method of operation, defendants' website no longer does such caching. (RT 111). Instead, a third party under contract to defendants performs that function. (RT 111). However, when a user runs a search on defendants' website, every search is a request on defendants' server. (RT 126). Similarly, when a user gets a list of results back, clicks one of those links, and gets taken to a detailed dot-torrent page hosted by defendants' server, all of those pages-on which the names of dot-torrent files are identified-are hosted on defendants' server. (RT 127).

^{FN12}. Defendant Parker testified that he was advised by a Panther representative that Panther does not have the capacity for full-server logging on all of its servers. (RT 75). Although plaintiffs argue that Panther can selectively log certain data, there is no evidence in the record as to whether Panther specifically has the capacity to log the Server Log Data in issue. (RT 177).

^{FN13}. In light of the change in the method of operation, and the timing thereof, as well as the other evidence in the record, the court

finds that defendants have the ability to manipulate at will how the Server Log Data is routed. Indeed, defendants represent that they could disengage and resume the functions currently performed by Panther if directed to log the Server Log Data in issue. (RT 72, 103-04).

D. Plaintiffs' Preservation Request

*4 On May 15, 2006, defendants sent a notice to plaintiffs' counsel formally reminding counsel and plaintiffs of their obligation to preserve all potentially discoverable evidence in their possession, custody or control related to the litigation, including all logs for the TorrentSpy website, and records of all communications between defendants and users of the website, including instant-messaging and other chat logs. (Pozza I Decl., Ex. H). This notice did not specifically request that defendants preserve Server Log Data temporarily stored only in RAM. Plaintiffs do not point to any other preservation request which specifically addresses data temporarily stored only in RAM. The court further notes that prior to the filing of Plaintiffs' Motion, the docket does not reflect that plaintiffs sought a preservation order.

IV. DISCUSSION

A. The Server Log Data in Issue 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. [F.R. Civ. P. 26\(b\)\(1\)](#). Plaintiffs argue that the Server Log Data is relevant to numerous claims and defenses, including whether defendants' users have directly infringed plaintiffs' copyrighted works, and to what extent defendants' website is used for purposes of copyright infringement. (Plaintiffs' Motion at 1, 15-20). The court agrees. This case is predicated on theories of vicarious infringement, contributory infringement, and inducement. (Complaint ¶¶ 34-36). Primary infringement is a necessary predicate to such claims. [Perfect 10, Inc. v. Amazon.com, Inc.](#), 487 F.3d 701, 2007 WL 1428632, *15 (9th Cir. May 16, 2007) (citing [A & M Records, Inc. v. Napster, Inc.](#), 239 F.3d 1004, 1013 n. 2) (9th Cir.2001)). Defendants contest primary infringement. (Answer ¶ 33). Indeed, defendant Parker's testimony suggests his view that

without logs, a case cannot be made against a website alleged to have engaged in secondary/contributory infringement because such logs are “essential” to finding direct infringers. (RT 129-30). There can be no serious dispute that the Server Log Data in issue is extremely relevant and may be key to the instant action.^{FN14}

^{FN14}. Defendants contend that plaintiffs' request for Server Log Data is overbroad because the vast majority of the website's users are located overseas such that their conduct cannot constitute copyright infringement. (RT 115-20, 125-26). The court rejects this contention. First, defendants' evidence regarding the volume of overseas traffic lacks foundation and is speculative at best. Second, even if defendants are correct regarding the asserted volume of overseas traffic, the court still finds such data to be relevant or reasonably calculated to lead to the discovery of relevant admissible evidence. Having said that, if (1) it is technically feasible; (2) defendants could reliably demonstrate that (i) Panther's United States servers process Server Log Data for users in the United States; and (ii) measures could be taken to protect against manipulation of the routing to alter the representative nature of such data; and (3) defendants choose to meet their obligations under this order by directing Panther to retain and provide defendants with the Server Log Data for dissemination to plaintiffs, the court would entertain a request to limit the required preservation and production to Server Log Data that is processed through the RAM of Panther's United States servers pursuant to its contract with defendants. Alternatively, if a reliable and verifiable means exists to identify the country from which requests to defendants' website for dot-torrent files originated, the court would entertain a request to limit the required preservation and production to Server Log Data originating from users of defendants' website in the United States. The court does not view the data provided on the optional registration surveys referenced by defendant Parker during his testimony as a reliable and verifiable means to identify the country from which user requests originate.

(RT 126).

B. The Server Log Data in Issue Is Electronically Stored Information

[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. [F.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.*

*5 Defendants argue that the Server Log Data does not constitute electronically stored information under [F.R. Civ. P. 34\(a\)](#) because the data has never been electronically stored on their website or in any medium from which the data can be retrieved or examined, or fixed in any tangible form, such as a hard drive. (Defendants' Supp. Memo I at 1; Parker II Decl. ¶ 2). Plaintiffs assert that the Server Log Data is electronically stored information because such data is copied to the RAM while user requests are processed. (Plaintiffs' Supp. Memo II at 2; Horowitz II Decl. ¶ 4).

Although the parties point to no cases in which a court has assessed whether data present only in RAM constitutes electronically stored information under [Rule 34](#), the Ninth Circuit has addressed whether data in RAM is electronically stored information in another context. In [MAI Systems 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.^{FN15} It 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.”).

FN15. The Ninth Circuit effectively reaffirmed the continuing viability of *MAI* in its recent opinion [Perfect 10, Inc. v. Amazon.com, Inc.](#), 487 F.3d 701, 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 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.](#), 487 F.3d 701, 2007 WL 1428632, at *6.

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](#). Based on the evidence in the record, the court finds that the Server Log Data in this case is transmitted through and

temporarily stored in RAM while the requests of defendants' website users for dot-torrent files are processed. Consequently, such data is electronically stored information under [Rule 34](#).

C. The Server Log Data in Issue Is within the Possession, Custody or Control of Defendants

[Rule 34\(a\)](#) is limited in its scope to documents and electronically stored information which are in the possession, custody or control of the party upon whom the request is served. [F.R. Civ. P. 34\(a\)](#); [Rockwell Int'l Corp. v. H. Wolfe Iron & Metal Co.](#), 576 F.Supp. 511, 512 (W.D.Pa.1983).

*6 Prior to the filing of Plaintiffs' Motion, the Server Log Data was received, at least in large part, in defendants' website's RAM, and therefore was clearly within defendants' possession, custody and control. As the Server Log Data is now directed to Panther's RAM as opposed to the RAM on defendants' website, the court must also consider whether the Server Log Data routed to Panther is in defendants' possession, custody or control.

Federal courts have consistently held that documents are deemed to be within a party's possession, custody or control for purposes of [Rule 34](#) if the party has actual possession, custody or control, or has the legal right to obtain the documents on demand. [In re Bankers Trust Co.](#), 61 F.3d 465, 469 (6th Cir.1995); see also [United States v. International Union of Petroleum and Industrial Workers, AFL-CIO](#), 870 F.2d 1450, 1452 (9th Cir.1989) (“Control is defined as the legal right to obtain documents upon demand.”). The record reflects that defendants have the ability to manipulate at will how the Server Log Data is routed. Consequently, the court concludes that even though the Server Log Data is now routed to Panther and is temporarily stored in Panther's RAM, the data remains in defendants' possession, custody or control.

D. 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, *2 \(C.D.Cal.2002\)](#) (citing [Alexander, 194 F.R.D. at 310](#)).

Defendants argue that because their website has never recorded or stored Server Log Data since the commencement of the website's operations, requiring defendants to retain such data would be tantamount to requiring them to create a record of the Server Log Data for its production. Plaintiffs contend that the Server Log Data already exists because such data is generated by the website users, received by a web server operated by, or under contract to defendants, and utilized to respond to user requests. As suggested by the court's analysis above, the court concludes that the Server Log Data in issue exists and, at least until recently, was temporarily stored in defendants' RAM.

As noted above, because the Server Log Data is temporarily stored in Panther's RAM, and is in the possession, custody or control of defendants, defendants would not be required to create new information for its production. 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, *2 \(C.D.Cal.2002\)](#) (denying production of customer data because such information “is not now and has never been in existence”); [Alexander v. FBI, 194 F.R.D. 305, 310 \(D.D.C.2000\)](#) (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 in RAM, 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.

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

*7 Plaintiffs' Motion requests that the court issue an order requiring defendants to preserve the Server Log Data. Plaintiffs contend, *inter alia*, that defendants are and have been obligated to preserve the Server Log Data, and that activating a logging function to

preserve and store the server log data would impose no undue burden or cost on defendants. 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 that requiring such preservation would be unduly burdensome.

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 the 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 the Server Log Data.

The third factor requires more analysis. The parties offer drastically different views regarding the degree to which defendants may be burdened if they are required to preserve the Server Log Data. As the “burden” issues relative to preservation significantly overlap with the “burden” issues relative to production, the court will address such issues together.

First, the court considers the potential burden attendant to employing a technical mechanism through which retention of the Server Log Data in RAM may be enabled. Plaintiffs contend that employing such a technical mechanism would be a trivial matter involving little more than a setting change on the web server program. (Horowitz I. Decl. ¶ 15). Defendants concede that the activation of a logging function to enable the retention of Server Log Data in RAM, in and of itself, would not be difficult. (Jt. Bunnell/Parker Decl. ¶ 7). Consequently, the court finds that it would not be an undue burden on defendants to employ a technical

mechanism through which retention of Server Log Data in RAM is enabled.^{FN16}

^{FN16}. The record also reflects that a programmatic method (which is distinct from enabling the logging function) could be employed to retain the Server Log Data from http headers while the data is in RAM. (RT 78, 81). Employing such a technique would require the writing of a script to collect the Server Log Data which would take several hours. (RT 78, 81). The court also find that the use of the programmatic method would not impose an undue burden on defendants.

Second, the court considers the potential burden attendant to actually retaining (*i.e.*, recording and storing) and producing the Server Log Data. Defendants contend that the burdens attendant to recording, storing and producing the Server Log Data would be technically, financially, and legally prohibitive. Plaintiffs disagree and argue that most of defendants' contentions are based on an incorrect premise and a vastly overbroad assumption regarding the scope and volume of data in issue.

(i) Volume of Data/Resulting Costs/Impact on Website Functionality

*8 Defendants represent that the Server Log Data would accumulate 30-40 gigabytes (30,000 to 40,000 megabytes) a day—a volume which defendants' current server does not have the capacity to record, store or copy, and the retention of which would negatively affect the functionality of their website, and require a costly re-design of their system and the installation of new equipment.^{FN17}(Jt. Bunnell/Parker Decl. ¶¶ 6, 8). Defendants further argue that the costs of producing such material would be prohibitive.^{FN18} However, during the hearing in this matter, it became evident that defendants' representation regarding the volume of Server Log Data was significantly overstated. Rather than estimating the volume of incoming Server Log Data only, defendants estimated the volume of *all* requests for data.^{FN19}(RT 60-62). On cross-examination, defendant Parker conceded that collecting and recording only the subset of Server Log Data would “most likely” result in a volume of data far less than 40 gigabytes (40,000 megabytes) a day. (RT 82). Plaintiffs' expert in fact testified that

the Server Log Data would likely have a volume of one-hundredth of what defendant Parker had originally suggested (*i.e.*, 300 to 400 megabytes).^{FN20} (RT 134). Defendant Parker testified that he had not considered data storage issues if the volume was significantly smaller, *i.e.*, if the Server Log Data in issue had a volume of only one gigabyte (1000 megabytes) a day.^{FN21}(RT 82-83). He did concede, however, that if the logging was limited to only the Server Log Data (as opposed to *all* incoming data), he would not have the same concerns about, *inter alia*, computer processing unit usage.^{FN22}(RT 86).

^{FN17}. Based on the (incorrect) assumption that the data to be preserved would have a volume of 30 to 40 gigabytes a day, defendants estimate that they would either need to redevelop their existing server at an estimated cost of \$10,000 and an expenditure of two weeks of time, or terminate their existing arrangement and set up a new higher capacity server system at an estimated cost of \$50,000. (Defendants' Supp. Memo II at 5; Jt. Bunnell/Parker Decl. ¶¶ 6, 8).

^{FN18}. Defendants contend that since they are not physically in the Netherlands where their server is located, saving the Server Log Data would require a File Transfer Protocol (“FTP”) download of the files from the server. (Jt. Bunnell/Parker Decl. ¶ 6). Based again on the (incorrect) assumption that the volume in issue is 30 to 40 gigabytes a day, defendants represent that it would be impossible to download this volume in a single download day. (Jt. Bunnell/Parker Decl. ¶ 6). Defendants argue that even if this volume of data could be burned onto a DVD, approximately 10 DVDs would need to be burned on a daily basis, and then shipped overseas, requiring an unreasonable amount of human labor time spent processing and burning the data. (Defendants' Supp. Memo II at 3; Jt. Bunnell/Parker Decl. ¶ 6).

^{FN19}. Defendant Parker testified that he based his estimate on the volume of logging “everything”—“every image, any kind of

thing that loads up to the user”-because he did not believe that the logging function could be selectively enabled to retain just the Server Log Data. (RT 60-62). The court does not accept defendant Parker's testimony regarding the inability to selectively enable logs to retain solely the Server Log Data in issue. Indeed, defendant Parker ultimately conceded, after reviewing an exhibit offered by plaintiffs, that the software used by defendants' website could create server logs for limited amounts of data and could save it in a particular folder. (RT 78). The court concludes that defendant Parker either did not know that the logs could be selectively enabled to collect the Server Log Data only or that he intentionally misrepresented the volume of data in issue. The former suggests a lack of knowledge and expertise which significantly undercuts his testimony. The latter suggests a lack of candor which likewise significantly undercuts his testimony. As the incorrect assumption that logs could not be selectively enabled serves as the predicate for virtually all of defendants' testimony and declarations regarding the alleged burden that would be imposed upon defendants if they were required to preserve and produce just the Server Log Data, such testimony and declarations are completely undercut and not viewed by this court as credible.

[FN20](#). Plaintiffs contend that even if the data generated a few gigabytes of storage space per day, the data could be backed up on a DVD, which can store up to four gigabytes of data and would take around five to ten minutes. (Horowitz Decl. ¶ 18). Plaintiffs further assert that storing the data would not be costly because a DVD can be purchased for under a dollar. (Horowitz Decl. ¶ 18).

[FN21](#). Defendant Parker also failed to consider that the volume of even just the Server Log Data would be further significantly reduced if compressed, or if collected in binary (rather than text) format. (RT 83-84, 135-36).

[FN22](#). Defendant Parker similarly indicated

that he would not have the same concerns if the programmatic method was limited to retention of only the Server Log Data (as opposed to all incoming data). (RT 86).

Based upon the evidence regarding the estimated volume of data resulting from the logging of solely the Server Log Data in issue (as opposed to all data) and the other evidence presented, the court finds that defendants would not be unduly burdened as a consequence of the volume of Server Log Data if required to preserve and produce such data.

(ii) Privacy/First Amendment/Federal Statutory Issues

Defendants also raise issues concerning the privacy of their website users based upon defendants' privacy policy, the First Amendment and multiple federal statutes. (Defendants' Supp. Memo II at 8-15). 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.[FN23](#) The court finds that defendants' asserted interest in maintaining the privacy of the users of their website can be adequately protected by the protective order already entered in this action and the masking of the users' IP addresses. See [Farber, 234 F.R.D. at 191](#).

[FN23](#). Although defendants suggest that the actual IP addresses could be retrieved from masked/encrypted IP addresses through “brute force,” the court has protected against that by prohibiting plaintiffs from taking any measures to unmask or decrypt the masked/encrypted IP addresses.

(a) Privacy Policy

Defendants contend that Plaintiffs' Motion should be denied because plaintiffs' privacy policy precludes them from preserving and producing “personal information” about their website's users. The court rejects this contention.

*9 First, defendants cannot insulate themselves from complying with their legal obligations to preserve and produce relevant information within their

possession, custody or control and responsive to proper discovery requests, by reliance on a privacy policy-the terms of which are entirely within defendants' control.

Second, even if a litigant's privacy policy could have such an impact, it is not clear to the court that defendants' current privacy policy actually prohibits the retention and production of the Server Log Data. *Seesupra* note 10. Moreover, the record reflects that despite this policy, defendants, unbeknownst to their users, do disclose IP addresses and search queries to third parties, albeit without disclosure of clicks on dot-torrent download links. (RT 90-97).

Third, to the extent defendants' privacy policy may prohibit the disclosure of IP addresses, compliance with this order does not violate such policy because IP addresses are to be masked.

Finally, even if the privacy policy currently prohibits the retention and disclosure of the Server Log Data, the policy itself advises users that such policy may be modified at any time. As this order does not contemplate the historical retention and production of data from users who have arguably relied on the existing policy, and as nothing in this order prevents defendants from modifying their privacy policy so that it accurately reflects defendants' prospective retention and production obligations pursuant to this order, defendants themselves retain the ability to ensure that they do not violate their own privacy policy.

(b) First Amendment

Defendants also argue that Plaintiffs' Motion should be denied because the First Amendment protects anonymous speech on the internet.

The First Amendment protects anonymous speech, at least in circumstances involving core First Amendment expression such as political speech. See *McIntyre v. Ohio Elections Commission*, 514 U.S. 334, 115 S.Ct. 1511, 131 L.Ed.2d 426 (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' website 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' website and that the IP addresses of such users have been ordered to be masked.

(c) Stored Communications Act

*10 Defendants 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. 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 an agent thereof; or (2) with the lawful consent of an intended recipient of such communication.^{FN24} 18 U.S.C. §§ 2702(b)(1), 2702(b)(3).

^{FN24}. As the cases upon which defendants rely involve third party subpoenas to electronic server providers who were not the intended recipients of the communications in issue, they are not applicable.

As defendants' website is the intended recipient of the Server Log Data, and defendants have the ability to consent to the disclosure thereof, this statutory provision does not provide a basis to withhold such data which is clearly within defendants' possession, custody and control.^{FN25}

^{FN25}. As the good faith reliance on a court order (such as the instant order) provides a complete defense to any civil or criminal action predicated on a violation of the above-referenced non-disclosure provision,

the court also rejects defendants' assertions of burden based on the potential of being sued for violating this provision. [18 U.S.C. § 2707\(e\)](#).

(d) The Wiretap Act

Defendants argue that Plaintiffs' Motion should be denied because the Wiretap Act ([18 U.S.C. §§ 2510-22](#)) prohibits the disclosure of the Server Log Data.

[Title 18, United States Code, Section 2511](#), generally prohibits the intentional interception of electronic communications during the transmission thereof and the disclosure of such intercepted communications. [18 U.S.C. §§ 2511\(a\), 2511\(c\), 2510\(12\)](#). [Title 18, United States Code, Section 2510\(12\)](#) defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photoptical system that affects interstate or foreign commerce" except as expressly excluded therein. Specifically excepted from the prohibition against the interception and disclosure of electronic communications are: (1) the interception by a party to the communication; (2) the disclosure of the contents of such communication while in transmission to the intended recipient of such communication or an agent thereof; and (3) the disclosure of the contents of such communication while in transmission with the lawful consent of an intended recipient of such communication. [18 U.S.C. §§ 2511\(2\)\(d\), 2511\(3\)\(a\), 2511\(3\)\(b\)\(ii\)](#).

First, the court concludes that this statute is not implicated because, as to electronic communications, it only prohibits interceptions during transmission (not while in electronic storage, *i.e.*, RAM), and the disclosure of electronic communications intercepted during transmission. See [Konop v. Hawaiian Airlines, Inc.](#), 302 F.3d 868, 878-79 (9th Cir.2002). This is true even though storage is a necessary incident to transmission. *Id.* at 879 n. 6.

Second, even if the Server Log Data were considered to be in transmission while in RAM, and therefore subject to this statute's prohibition against interception and disclosure, the statute would still not relieve defendants of their obligation to preserve and produce such data. As defendants' website is the

intended recipient of the Server Log Data, and defendants can lawfully intercept and consent to the disclosure thereof, this statutory provision, even if applicable would not provide a basis to withhold such data which is clearly within defendants' possession, custody and control.^{FN26}

^{FN26}. As the good faith reliance on a court order (such as the instant order) provides a complete defense to any civil or criminal action predicated on a violation of the above-referenced non-disclosure provision, the court also rejects defendants' assertions of burden based on the potential of being sued for violating this provision. [18 U.S.C. § 2520\(d\)\(1\)](#).

(e) The Pen Register Statute

*11 Defendants also argue that Plaintiffs' Motion should be denied based on the Pen Register Statute ([18 U.S.C. §§ 3121-27](#)).

[Title 18, United States Code, Section 3121](#), generally prohibits the installation and use of pen registers and trap and trace devices except in the circumstances referenced therein. [18 U.S.C. § 3121\(a\)](#). A pen register is essentially a device which captures outgoing telephone numbers or IP addresses.^{FN27} A trap and trace device essentially captures incoming IP addresses or telephone numbers (such as a caller identification device).^{FN28} Excepted from this prohibition are pen register and trap and trace devices used by providers of electronic communication services relating to the operation and maintenance of such service. [18 U.S.C. § 3121\(b\)\(1\)](#).

^{FN27}. More specifically, a pen register is a device or process which records dialing, routing, addressing or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, excluding the contents of any communication. [18 U.S.C. § 3127\(3\)](#). Such term does not include (i) any device or process used by a provider of electronic communication service for billing, recording as an incident to billing, or providing communications services; or (ii) any device or process used by such provider for cost accounting or other like purposes in the

ordinary course of its business. [18 U.S.C. § 3127\(3\)](#).

[FN28](#). More specifically, a “trap and trace device” is a device or process which captures the incoming electronic or other impulses which identify the originating number of an electronic communication, excluding the contents of any communication. [18 U.S.C. § 3127\(4\)](#).

As the Server Log Data sought by plaintiffs encompasses incoming IP addresses, it arguably implicates the prohibition against the unauthorized use of trap and trace devices. However, as plaintiffs correctly note, the collection of incoming IP addresses by defendants is exempt from this prohibition pursuant to [18 U.S.C. § 3121\(b\)\(1\)](#) because defendants already and necessarily capture such data in their RAM (or Panther's RAM) to operate the website.

(f) Impact on Good Will

Defendants also argue that they would lose business and good will of customers and advertisers as result of the stigma that would flow from any order directing them to preserve and produce the Server Log Data. (Jt. Bunnell/Parker Decl. ¶ 9; RT 152-55).

The testimony and declarations of defendants Parker and Bunnell regarding such loss of good will and business is largely speculative, conclusory and without foundation.^{[FN29](#)} 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' website is perceived by its users and advertisers and result in a loss of business and good will. Notably, these concerns did not prevent the court in *Gonzales* from ordering a third party to disclose certain data to the United States government.

[FN29](#). For example, although defendant Bunnell testified that the sites Grokster and Lokitorrent “were basically shut down” because they were “forced to turn over log information” (RT 153), on cross-examination, it became clear that he did not have any personal knowledge regarding

such matters and that his testimony was, at most, based on things he had read or heard which might or might not be true. (RT 159-62). Similarly, defendant Bunnell provided a declaration and testified regarding his concern about suffering the same type of consequences as AOL, which defendants contend was sued because it published search queries and log-in information excluding IP addresses on the internet. (RT 153-54). However, it again became clear during cross-examination that defendant Bunnell's testimony was speculative and without foundation. Indeed, although a copy of a complaint against AOL was attached to and referenced in his declaration, Bunnell apparently did not even realize that the testimony he was providing about such lawsuit related to said complaint as he both denied having read it and then affirmed having read it. (RT 163-65). The court observes, based on its review of the copy of the complaint against AOL that is of record, that the data in issue in that case, unlike the Server Log Data in issue here, encompassed personal identifying user names, street addresses, dates of birth, phone numbers, credit card numbers, and social security numbers. (Jt. Bunnell/Parker Decl., Ex. C). The AOL case also does not appear to have involved disclosure pursuant to a court order as contemplated in the instant case. (Jt. Bunnell/Parker Decl., Ex. C).

In this case involving the preservation and disclosure by a party to another private civil litigant, the court finds that 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 and business, 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.^{[FN30](#)}

[FN30](#). 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. 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."

In light of fact that the Server Log Data is currently routed to Panther, the court has also considered whether a third party discovery request to Panther would be a viable alternative. The court concludes that while such data may well be obtainable from Panther, requiring plaintiffs to pursue that avenue would likely not be "more convenient, less burdensome, or less expensive" in light of the nature of the relationship between defendants and Panther, the nature of the information sought, and the other evidence presented in this matter.

(iii) International Issues

Defendants further assert that any changes to the existing web server would need to be in compliance with Netherlands law because defendants lease their server from an Internet Service Provider in Amsterdam, Netherlands and their server is located at the ISP's secure plant. (Defendants' Supp Memo II at 2; Jt. Bunnell/Parker Decl. ¶ 6). Defendants have offered evidence that defendants' contract with the entity from which it leases its Netherlands server is governed by Netherlands law. (Jt. Bunnell/Parker Decl., Ex. A). Defendants have also supplied the court with the Netherlands Personal Data Protection Act which is directed to "information relating to an identified or identifiable person."(Jt. Bunnell/Parker Decl., Ex B). The court is not persuaded that such concerns should relieve defendants of their obligation to preserve and produce the Server Log Data.

***12** First, as it now appears that the entity which has immediate possession of the Server Log Data has over 25 United States servers, defendants' expressed international concerns no longer appear valid. At a minimum, their expressed concerns carry less weight in light of their use of Panther's services and the fact that defendants retain the ability to manipulate the routing of the Server Log Data.

Second, even if such concerns remain, it is not clear that the Netherlands' Personal Data Protection Act applies to IP addresses, let alone to the other Server Log Data in issue, as an IP address identifies a computer, rather than a specific user of a computer. *Seesupra* note 7. A party relying on 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.

Third, even if the Netherlands' statute applies and is read to prohibit defendants' preservation or production of the Server Log Data, 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 (let alone preserve) 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 concludes that these factors weigh in favor of requiring defendants to preserve and produce the Server Log Data. The court primarily relies upon the key relevance of the Server Log Data to this action, the specificity of the data sought, the lack of alternative means to acquire such information, and the fact that defendants are United States individuals and entities who affirmatively chose to locate their server in the Netherlands at least in part to take advantage of the perceived protections afforded by that country's information security law.

*13 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.

F. An Order Requiring the Production of Certain 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. [F.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 F.R. Civ. P. (b)(2)(C). A court may limit discovery of electronic materials under [F.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. [F.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. [FN31](#)

[FN31](#). The court emphasizes that its ruling should *not* be read to require litigants in all cases to preserve and produce electronically stored information that is temporarily stored only in RAM. The court's decision in this case to require the retention and production of data which otherwise would be temporarily stored only in RAM, is based in significant part on the nature of this case, the key and potentially dispositive nature of the Server Log Data which would otherwise be unavailable, and defendants' failure to provide what this court views as credible evidence of undue burden and cost.

G. 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 13-14).

Pursuant to [F.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. [F.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](#).

*14 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-tapes, which may continue to be recycled on the schedule set forth in the company’s policy. *See id.*

As noted above, although this court now finds that defendants have an obligation to preserve the Server Log Data in issue that is temporarily stored only in RAM, in the absence of (1) prior precedent directly on point in the discovery context; (2) a specific request by defendants to preserve Server Log Data present solely in RAM; and (3) a violation of a preservation order, this court finds that defendants’ failure to retain the Server Log Data in RAM was based on a good faith belief that preservation of data temporarily stored only in RAM was not legally required. Consequently, the court finds that evidentiary sanctions against defendants for spoliation of evidence are not appropriate.

H. Attorneys’ Fees and Costs

Defendants request that the court require plaintiffs to pay reasonable expenses incurred in opposing Plaintiffs’ Motion, including attorneys’ fees, pursuant to F.R. Civ. P. 37(a)(4)(B). As Plaintiffs’ Motion has largely been granted, the court finds that the award of such fees is not appropriate. To the extent Plaintiffs’ Motion has been denied in part, the court finds that the making of such motion was substantially justified and that the award of expenses would be unjust.

V. CONCLUSION

Based upon the foregoing, IT IS HEREBY ORDERED:

1. Defendants are directed to commence preservation of the Server Log Data in issue within seven (7) days of this order and to preserve the Server Log Data for the duration of this litigation or until further of this court or the assigned District Judge. As the record reflects that there are 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.

2. Defendants shall initially produce 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.^{FN32} Although defendants are required to preserve the IP addresses of the computers used to request dot-torrent files, defendant 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.^{FN33} Plaintiffs are prohibited from using “brute force” or any other 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’ website of the fact that the Server Log Data is being preserved and has been ordered produced with masked/encrypted/redacted IP addresses.^{FN34}

^{FN32}. Plaintiffs have represented that they are willing to accept a sample of Server Log Data of one hour a day, provided that the hour each day is selected to provide a representative picture of the usage of defendants’ site. (RT 180-81). The court has not limited its order to sampling at this juncture because of concerns that one hour a day will not provide a representative sample of activity in light of defendants’ expressed concerns regarding its notification and disclosure obligations vis-a-vis its 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.

[FN33](#). 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, defendants’ production should reflect that “abcd.efgh.ijkl” made the request on day two at noon as well as on day one at noon.

[FN34](#). Having said that, absent further order of this court or the assigned District Judge, the Clerk is directed to file and maintain this order *underseal* for a period of seven (7) days. The court finds good cause to file such order *underseal* for at least the limited seven-day period in light of the nature of its contents and the fact that it may be based, at least in part on materials submitted *underseal* 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.

*15 3. Plaintiffs’ request for evidentiary sanctions based upon plaintiffs’ failure to date to preserve the Server Log Data is denied.

4. Defendants’ request for attorneys’ fees and costs pursuant to [F.R. Civ. P. 37\(a\)\(4\)\(B\)](#) is denied.

IT IS SO ORDERED.

C.D.Cal.,2007.

Columbia Pictures Industries v. Bunnell
Not Reported in F.Supp.2d, 2007 WL 2080419
(C.D.Cal.)

END OF DOCUMENT