P Send

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

COLUMBIA PICTURES, INC., et al.,

Plaintiffs,

vs.

JUSTIN BUNNELL, et al.,

Defendants.

2: 06-cv-01093 FMC-JCx

ORDER DENYING DEFENDANTS' MOTION FOR REVIEW

#254

This matter is before the Court on Defendants' Objections to and Motion for Review of Order Regarding Server Log Data (docket no. 194), filed June 12, 2007. The Court has read and considered the moving, opposition, and reply documents submitted in connection with this motion. The matter was heard on August 20, 2007, at which time the parties were in receipt of the Court's Tentative Order. For the reasons and in the manner set forth below, the Court hereby **DENIES** Defendants' Motion.

//

//

//

//

FACTUAL BACKGROUND AND PROCEDURAL HISTORY

Plaintiffs are motion picture studios that own copyrights or exclusive reproduction and distribution rights to numerous movies and television programs. Defendants operate a website that serves as a search engine that enables users to locate and download dot-torrent files. Using dot-torrent files and an independent computer software program, a "BitTorrent" client, users join a peer-to-peer network that facilitates the copying and distribution of the files that were the subject of the users' search. Defendants' website thereby allegedly permits Internet users to locate and download, view, store, and distribute unauthorized copies of Plaintiffs' copyrighted motion pictures and television shows. In this way, Plaintiffs allege Defendants knowingly enable, encourage, induce, and profit from the online piracy of Plaintiffs' copyrighted works.

On February 23, 2006, Plaintiffs filed a Complaint asserting a claim for copyright infringement. Numerous discovery disputes have arisen between the parties, and Defendants have repeatedly moved this Court to review and reconsider the rulings of Magistrate Judge Chooljian. On June 12, 2007, Defendants filed their latest challenge, against the Magistrate Judge's May 29, 2007, 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 (the May 29 Order), on June 12, 2007.

STANDARD OF LAW

A district court will not modify or set aside a magistrate judge's order unless it is "found to be clearly erroneous or contrary to law." Fed. R. Civ. P. 72(a).[1] The clearly erroneous standard applies to the magistrate judge's factual

[1] In addition, the Local Rules require that a party objecting to a Magistrate

findings while the contrary to law standard applies to the magistrate judge's legal conclusions, which are reviewed de novo. *See Wolpin v. Philip Morris, Inc.*, 189 F.R.D. 418, 422 (C.D. Cal. 1999); *see also Center for Biological Diversity v. Federal Highway Admin.*, 290 F. Supp. 2d 1175, 1199-1200 (S.D. Cal. 2003) (quoting *Weeks v. Samsung Heavy Indus. Co., Ltd.*, 126 F.3d 926, 943 (7th Cir. 1997), for the proposition that "discretionary orders and will be overturned 'only if the district court is left with the definite and firm conviction that a mistake has been made'").

When reviewing discovery disputes, however, "the Magistrate is afforded broad discretion, which will be overruled only if abused." *Wright v. FBI*, 385 F. Supp. 2d 1038, 1041 (C.D. Cal. 2005); *Geophysical Sys. Corp. v. Raytheon Co., Inc.*, 117 F.R.D. 646, 647 (C.D. Cal. 1987) (Tashima, J.) (questions of relevance in discovery context are reviewed under "the clearly implicit standard of abuse of discretion.").

DISCUSSION

I. The Scope of Federal Rule of Civil Procedure 34

At the heart of Defendants' Motion for Review is the following question of first impression: is the information held in a computer's random access memory (RAM) "electronically stored information" under Federal Rule of Civil Procedure 34?

Defendants and *amici* seek to engraft on the definition of "stored" an additional requirement, that the information be not just stored, but stored "for later retrieval." They argue that "electronically stored information" cannot

---

Judge's ruling on a nondispositive matter must "designat[e] the specific portions of the ruling objected to and stat[e] the grounds for the objection." Local Rule 72-2.1.

include information held in RAM because the period of storage, which may be as much as six hours, is too temporary. The Court finds this interpretation of "stored" unsupported by the text of the Rule, the accompanying commentary of its drafters, or Ninth Circuit precedent involving RAM. The Court holds that data stored in RAM, however temporarily, is electronically stored information subject to discovery under the circumstances of the instant case.

First, even the definition *amici* supplied fails to support their argument that information written to and held in random access memory is not "stored." As *amici* explain, according to the Merriam-Webster Collegiate Dictionary, to store means "to lay away, to accumulate or to place or leave in a location (as a warehouse, library, or *computer memory*) for preservation *or later use or disposal*." *Merriam-Webster's Collegiate Dictionary* (Frederick C. Mish et al. eds., 10th ed. 1993) (emphasis added). It is undisputed that RAM is computer memory and that information held in RAM is held there for later use by the computer (e.g., to be used in tasks performed by software or written to a hard drive, flash drive, DVD, or other more permanent medium) or disposal (e.g., to be erased when the computer is turned off or when the data is overwritten with new information as part of the regular computing process).

The definition of "to store" from the Random House Dictionary of the English Language specific to the context of computers further undermines Defendants' argument that RAM does not store data: "13. *Computers*. to put *or* retain (data) in a memory unit." Random House dictionary of the English Language (Stuart B. Flexner et al. eds., 2d ed. 1987) (emphasis added). Under this definition, the information need not even be subsequently accessed or used; simply placing the data in the RAM module is sufficient for it to constitute electronically stored information.

In addition, RAM itself is *defined* as a storage unit, and, due to its speed relative to hard disk drives, is typically used as the computer's primary storage:

"Random Access Memory (RAM): A read/write, nonsequential-access memory used for the *storage* of instructions and data. Note 1: RAM access time is essentially the same for all storage locations. Note 2: RAM is characterized by a shorter access time than disk or tape storage." National Communications System, *Federal Standard 1037C: Telecommunications: Glossary of Telecommunication Terms* (Gen. Servs. Admin., 4th ed. 1996) (emphasis added). Accordingly, information held in RAM is "stored" under the plain meaning of the unambiguous language of Rule 34.

Second, the Notes of the Advisory Committee to the 2006 Amendments to Rule 34, which amended the Rule to make explicit that it authorized discovery of information stored electronically,[2] indicate that the definition was intended to be read expansively to include all current and future electronic storage mediums:

> The wide variety of computer systems currently in use, and the rapidity of technological change, counsel against a limiting or precise definition of electronically stored information. Rule 34(a)(1) is *expansive* and includes *any type of information that is stored electronically*. A common example often sought in discovery is electronic communications, such as e-mail. The rule covers--either as documents or as electronically stored information--information "stored in any medium," to encompass future developments in computer technology. Rule 34(a)(1) is intended to be *broad enough to cover all current types of computer-based information*, and flexible enough to encompass future changes and developments.

Fed. R. Civ. P. 34(a)(1) (2006 amendments) advisory committee's note. Such

---

[2] Rule 34(a) states, in part, that "[a]ny party may serve on any other party a request . . . to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect, copy, test, or sample *any* designated 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*--translated, if necessary, by the respondent into reasonably usable form, or to inspect, copy, test, or sample any designated tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served." Fed. R. Civ. P. 34(a) (emphasis added).

clear evidence that Rule 34(a)'s scope was intended to be as broad as possible, and cover data stored "in any medium from which information can be obtained," leaves no room to interpret the Rule to categorically exclude information written in a particular medium simply because that medium stores information only temporarily. Information in the RAM of Defendants' computers "can be obtained" by Defendant. It is undisputed that the Server Log Data[3] Plaintiffs seek can be copied from RAM in Defendants' computers and produced to Plaintiffs. Rule 34 requires no greater degree of permanency from a medium than that which makes obtaining the data possible. As information can be obtained from RAM, it is within the scope of Rule 34 and subject to discovery under the appropriate circumstances.

Finally, as discussed in the Magistrate Judge's May 29 Order, *amici* and Defendants' argument that data in RAM is too ephemeral to satisfy Rule 34's storage requirement is foreclosed by the Ninth Circuit's decision in *Mai Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993). To determine if the plaintiff could prevail on a claim of copyright infringement, the court in *Mai Systems Corp.* confronted the question of whether a program in RAM was "fixed in a tangible medium of expression," which the applicable statute defined as "sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration." *Id.* at 517-518; 17 U.S.C. § 101. Despite the Copyright Act's explicit requirement that the medium store information with a degree of permanence and for "more than transitory duration," the court held that a computer's copying of software into

---

[3] Server Log Data, as defined in the May 29 Order, includes (1) the anonymous (masked or encrypted) Internet Protocol (IP) address of users of Defendants' website who request dot-torrent files, (2) the identity of the dot-torrent files requested, and (3) the dates and times of such requests. (May 29 Order, 3:16-4:1.)

RAM was sufficient to meet the statutory prerequisites for liability and affirmed the district court's grant of summary judgment and issuance of a permanent injunction. *Id.* at 519.

In light of the Ninth Circuit's holding that RAM is a tangible medium, sufficiently permanent to permit reproduction, *amici* and Defendants' argument that RAM holds data for such a short duration that it is not stored subject to later access and retrieval simply has no merit. Defendants have therefore failed to establish that the Magistrate Judge's legal conclusion that data held in the RAM of computers under Defendants' control is within the scope of discoverable information under Federal Rule of Civil Procedure 34 was contrary to law.

In response to *amici*'s concerns over the potentially devastating impact of this decision on the record-keeping obligations of businesses and individuals, the Court notes that this decision does not impose an additional burden on any website operator or party outside of this case. It simply requires that the defendants in this case, as part of this litigation, *after* the issuance of a court order, and following a careful evaluation of the burden to these defendants of preserving and producing the specific information requested in light of its relevance and the lack of other available means to obtain it, begin preserving and subsequently produce a particular subset of the data in RAM under Defendants' control.

II. The Magistrate Judge's Authority to Order the Requested Discovery

In an attempt to resist complying with the Magistrate Judge's May 29 Order, Defendants have raised a number of creative legal challenges, the first of which is that the Magistrate Judge exceeded her authority by issuing an injunction and disposing of ultimate issues in the case. The Federal Magistrates Act provides that a magistrate judge may "hear and determine any pretrial matter pending before the court, except a motion for injunctive relief ," and seven other enumerated motions. 28 U.S.C. § 636(b)(1)(A). The Ninth Circuit has held that

the list of excluded motions is not exhaustive, and courts must "look to the effect of the motion, in order to determine whether it is properly characterized as dispositive or non-dispositive of a claim or defense of a party." *United States v. Rivera-Guerrero*, 377 F.3d 1064, 1068 (9th Cir. 2004). If it is a final order, dispositive of a claim or defense, it is outside of the magistrate's statutorily granted jurisdiction. *Id.* at 1069.

Plaintiffs' Motion to Require Defendants to Preserve and Produce Server Log Data and for Evidentiary Sanctions was neither a motion for injunctive relief nor its functional equivalent, and the May 29 Order granting the motion did not dispose of any of Defendants' claims or defenses. The May 29 Order is a quotidian discovery order, resolving disputes over relevance, burden, and the proper scope of discovery, that is well within the Magistrate Judge's authority and substantial specialized expertise. Magistrate judges regularly compel production of documents and, although courts in other jurisdictions have interpreted orders to preserve evidence as injunctions, the Ninth Circuit has held that all parties are under a duty not to intentionally dispose of evidence they know is relevant. *Idaho Potato Comm'n v. G&T Terminal Packaging, Inc.*, 425 F.3d 708, 720 (9th Cir. 2005); *Pueblo of Laguna v. United States*, 60 Fed. Cl. 133, 138 (2004) (holding that "a document preservation order is no more an injunction than an order requiring a party to identify witnesses or to produce documents in discovery.") (citing *Mercer v. Magnant*, 40 F.3d 893, 896 (7th Cir. 1994); *cf. Madden v. Wyeth*, No. 3-03-CV-0167-R, 2003 U.S. Dist. LEXIS 6427, at *1 (N.D. Tex. Apr. 16, 2003) ("A motion to preserve evidence is an injunctive remedy and should issue only upon an adequate showing that equitable relief is warranted.").

Moreover, contrary to Defendants' contentions, the May 29 Order does not dispose of any of Defendants' potential First Amendment or other defenses to Plaintiffs' claim for copyright infringement. The May 29 Order addresses only

Defendants' arguments in opposition to the requested discovery, not whether the First Amendment or the Electronic Communications Privacy Act (ECPA) might factor into a final, permanent injunction prohibiting Defendants from engaging in any form of copyright infringement. That the creation of a server log might be a predicate step in fashioning effective hypothetical final relief does not alter the fact that such final disposition of any of the parties' claims or defenses remains a future event. As the May 29 Order is not dispositive of any claims or defenses, it was within the Magistrate Judge's jurisdiction, and the Court overrules Defendants' objection.

III. The Fifth Amendment

Defendants argue that the Magistrate Judge violated their Fifth Amendment due process rights by (1) finding that they voluntarily consented to the disclosure of the Server Log Data and (2) ruling against Defendants based on their failure to demonstrate that there are alternative means of acquiring the requested information after denying Defendants' discovery requests that would have led to the production of data Defendants could use to demonstrate such means. Defendants have not provided any authority for the proposition that a magistrate's order could violate a defendants' Fifth Amendment rights or that a motion for review would be the proper venue for obtaining relief for such a hypothetical constitutional injury. Nevertheless, the Court will briefly address Defendants' arguments, construing them as arguments that the Magistrate Judge's factual findings were clearly erroneous and that her legal conclusions were contrary to law, the applicable legal standard.

Defendants contend that production of their Server Log Data would violate the Stored Communications Act (SCA), the Wiretap Act, and the Pen Register Statute. The SCA prohibits unlawful access to stored communications, which is defined as either "(1) intentionally access[ing] without authorization a facility through which an electronic communication service is provided; or (2)

intentionally exceed[ing] an authorization to access that facility; and thereby obtain[ing] . . . authorized access to a wire or electronic communication while it is in electronic storage in such system . . . ." The May 29 Order, however, contemplates no *unauthorized* access. Defendants are not ordered to access the facility of a third party and obtain stored communications, such as e-mails stored on a remote server. Defendants are also not custodians of private communications, as an Internet Service Provider would be of e-mails sent through its servers (where neither the sender nor the recipient would be parties to the litigation), ordered to disclose the contents of those communications. *Cf. Theofel v. Farey-Jones*, 341 F.3d 978, 985 (9th Cir. 2003). Rather, Defendants are the intended recipients of the information contained in the Server Log Data. When users access Defendants' website and request information (such as dot-torrent files), they voluntarily supply their IP addresses and a packet of information containing their request. That information is received and processed in Defendants' RAM on their servers, for their use (which, in addition to the contemporaneous fulfillment of the request, the record reveals has thus far consisted primarily of disclosure to advertisers to generate revenue). (May 29 Order 22:1-3; Reporter's Transcript of the April 3, 2007, Discovery Hearing (RT) 90-97).) Defendants' access to Defendants' information on servers under Defendants' control does not constitute unauthorized access to a "facility through which an electronic communication service is provided" or "to a wire or electronic communication while it is in electronic storage in such system." Production of the Server Log Data would therefore not violate the SCA.

The Wiretap Act makes it an offense to "intentionally intercept[] . . . any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). The Wiretap Act and the SCA are both part of the ECPA, and play complementary roles in Congress's regulatory scheme. Under the ECPA, an electronic communication may either be intercepted and actionable under the Wiretap Act or acquired while

in electronic storage and actionable under the SCA, but not both. *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 877 (9th Cir.2002). As such, an electronic communication may not simultaneously be actionable under both the Wiretap Act and the SCA. *Id.* The Ninth Circuit has held that the Wiretap Act applies only to "acquisition contemporaneous with transmission," and that "Congress did not intend for 'intercept' to apply to electronic communications when those communications are in 'electronic storage.'" *Theofel,* 359 F.3d at 1077-78, quoting *Konop.* 302 F.3d at 877. Communications are in "electronic storage" under the SCA, and outside the scope of the Wiretap Act, even where the storage is transitory and lasts for only a few seconds. *Quon v. Arch Wireless Operating Co.*, 445 F. Supp. 2d 1116, 1135-36 (C.D. Cal. 2006) (citing *Konop*, 302 F.3d at 878 n.6). As discussed above, the Server Log Data exists in electronic storage. The Wiretap Act is therefore inapplicable and does not pose any barrier to Defendants' compliance with the May 29 Order.

The Pen Register Statute is similarly inapplicable to the ordered discovery, as Defendants' own Motion makes clear. After discussing why the exemption the to the Pen Register Statute's prohibitions on use of pen registers and tap and trace devices that the Magistrate Judge relied upon does not apply in these circumstances, Defendants argued that the Court could not authorize production of the Server Log Data under the Pen Register Statute because the Server Log Data contains "contents" of communications, such as the identity of the dot-torrent files requested. As Defendants note, pen registers and trap and trace devices, by definition, do not record "the contents of any communication." 18 U.S.C. § 3127(3)–(4); *see also In re United States for an Order Authorizing the Use of a Pen Register & Trap*, 396 F. Supp. 2d 45, 50 (D. Mass. 2005) (interpreting "contents of communications" to include "application commands, search queries, requested file names, and file paths"). Because the May 29 Order requires the production of the contents of communications, Defendants have not

been ordered to install a pen register or trap and trace device, and the Pen Register Statute does not bar the ordered discovery. Accordingly, the Magistrate Judge's decision that production of the Server Log Data would not violate the SCA, the Wiretap Act, or the Pen Register Statute was not contrary to law.[4]

Defendants argue that the Magistrate Judge improperly based a number of key rulings on their failure to "prove facts where they could not obtain the needed evidence" because of the Magistrate Judge's prior rulings, and the orders of this Court, which concluded that the discovery Defendants were requesting would not lead to relevant or admissible evidence.

For example, Defendants note that the Magistrate Judge concluded 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." Defendants argue they were not able to present evidence of "alternative means to obtain such data" because "the evidence needed for such proof has been concealed by Plaintiffs in an institutional citadel of privilege." (Mot. 41:1-2.)

First, contrary to Defendants' arguments that "the Magistrate Judge's Order implicitly casts the burden of proof onto Defendants," in each instance Defendants cite, the decision is based on the Magistrate Judge's factual findings after a review of the full record that there were no "reasonable alternative means to obtain such data," not on Defendants' "failure to prove" the availability of any alternative means. Second, with respect to two of three challenged findings (the Magistrate Judge's determination that the requested production would not be

---

[4] As the Court's holding rests on independent legal grounds, it is unnecessary to review the Magistrate Judge's determination that Defendants' website constitutes an "electronic communications service."

unduly burdensome and that international law did not prohibit the requested discovery), the burden *was* properly on Defendants to demonstrate why they should be relieved from producing relevant information.

Finally, as discussed in this Court's prior orders, the information that was the subject of Defendants' denied discovery requests was irrelevant. Even if Defendants were able to show, as they allege, that Plaintiffs operate "honeypots" and participate in BitTorrent "swarms," thereby acquiring the IP addresses of individual copyright infringers, such evidence would not help them to demonstrate that "reasonable alternative means to obtain" the Server Log Data were available. Although Plaintiffs may have other means of discovering the IP addresses of individual direct infringers, in order to prevail in this action, Plaintiffs will need to establish that *Defendants* were in some way responsible for the direct infringement of others. The Server Log Data will show that individuals access Defendants' website and request and download dot-torrent files, which can be used to obtain Plaintiffs' copyrighted works without permission. This link in the causal chain is essential to proving Defendants' responsibility for copyright infringement under theories of contributory infringement, vicarious infringement, and inducement. Accordingly, the Magistrate Judge's finding of a "lack of a reasonable alternative means to obtain" the Server Log Data was not clearly erroneous or contrary to law.

IV. The First Amendment

Defendants argue that the Magistrate Judge's rejection of Defendants' First Amendment objections to the requested discovery was contrary to law because Plaintiffs failed to demonstrate a need for the Server Log Data and because the Magistrate Judge failed to perform a proper balancing test. The Court has already discussed why the Magistrate Judge's finding that Plaintiffs had a need for the Server Log Data was not clearly erroneous or contrary to law. The Court also agrees with the Magistrate Judge that "the preservation and disclosure of the

Server Log Data does not encroach or substantially encroach" upon the limited First Amendment protection to which the users of Defendants' website are entitled, "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." (May 29 Order 23:3-7.)

Defendants argue that, under *Adolph Coors Co. v. Wallace*, 570 F. Supp. 202, 208 (N.D. Cal. 1983), the Magistrate Judge was required to employ a formal three-part balancing test in determining whether to order the requested discovery. *Adolph Coors Co.*, in addition to not constituting binding precedent, proposed only that "any tribunal confronted with facts and arguments similar to those presented here undertake a sensitive evaluation in three steps." *Id.* In *Adolph Coors Co.*, the defendant Solidarity was a political organization comprised exclusively of gay men and lesbian women who sought to exert pressure on the plaintiff brewing company through a boycott in an effort to modify the plaintiff's political positions. *Id.* at 204. The plaintiff requested a list of the names of Solidarity's members and its sources of financial support. *Id.* Solidarity argued that revealing the group's members and donors would chill its associational privacy and freedom of political expression. *Id.*

In the instant case, Plaintiffs have sought data that would demonstrate that anonymous individuals accessed Defendants' website and requested dot-torrent files. Plaintiffs are not requesting the names or other identifying information, as the plaintiff sought in *Adolph Coors Co.*, and the May 29 Order ensures that such identifying information will not be disclosed. In addition, in contrast to the strong First Amendment protections for the freedom of association and right to engage in political speech, the privacy interests of Defendants' users are, at best, limited. To the extent the users are engaged in copyright infringement, the First Amendment affords them no protection whatsoever. *Harper & Row, Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 559, 105 S. Ct. 2218; 85 L. Ed. 2d 588

(1985) ("The essential thrust of the First Amendment is to prohibit improper restraints on the *voluntary* public expression of ideas; it shields the man who wants to speak or publish when others wish him to be quiet. There is necessarily, and within suitably defined areas, a concomitant freedom *not* to speak publicly, one which serves the same ultimate end as freedom of speech in its affirmative aspect.") (emphasis in original) (internal quotations omitted)); *A&M Records v. Napster, Inc.*, 239 F.3d 1004, 1028 (9th Cir. 2001) (holding that the First Amendment does not protect use of a peer-to-peer file sharing network that constitutes copyright infringement). Even if the users are engaged in *legal* file sharing, they have little to no expectation of privacy because they are broadcasting their identifying information to everyone in the BitTorrent "swarm" as they download the file. *See, e.g., In re Verizon Internet Servs.*, 257 F. Supp. 2d 244, 267 (D.D.C. 2003) (finding that "if an individual subscriber opens his computer to permit others, through peer-to-peer file-sharing, to download materials from that computer, it is hard to understand just what privacy expectation he or she has after essentially opening the computer to the world."). Similarly, because users openly disclose their IP addresses as part of the BitTorrent file transfer process, the Court is not persuaded by Defendants' argument that the retention of the IP addresses of users who obtain dot-torrent files from Defendants' website will "chill" their speech. Accordingly, the Court is satisfied that the Magistrate Judge properly weighed Defendants' First Amendment concerns against the need for the requested discovery, and that her resolution of the matter was not contrary to law.

V. Impact of International Law

Defendants insist that the Magistrate Judge erred in rejecting their argument that the law of the Netherlands, where Defendants have placed their servers, prohibits the courts of the United States from ordering the requested discovery in this action. First, the Magistrate Judge properly found that

Defendants had failed to meet their burden in establishing that Netherlands law would prohibit retention of the Server Log Data or production of an encrypted, anonymous version of that data to Plaintiffs. *See United States v. Vetco, Inc.*, 691 F.2d 1281, 1289 (9th Cir. 1981) ("The party relying on foreign law has the burden of showing that such law bars production."). Defendants argue the Magistrate Judge erred, citing a recent opinion of the Amsterdam District Court that held as follows:

> A service provider may, in certain circumstances, be obliged to provide rights holders (or their representatives) with the information asked for. For this, the Court must first of all be satisfied that there have been (unlawful) infringement activities by the subscribers concerned and, secondly, that it is beyond reasonable doubt that those whose identifying information is made available are also actually those who have been guilty of the relevant activities.

BREIN Foundation v. UPC Nederland B.V., Fabrizio Decl. Ex. 28. As the quoted text makes evident, however, *BREIN Foundation* does not support Defendants' argument. It places restrictions only on the production of "identifying information." As the Server Log Data Defendants must produce is anonymous, *BREIN Foundation*, even if it were the applicable legal standard, would not prohibit its production.

Second, as the Supreme Court has stated, "[i]t is well settled that [foreign] 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." *Societe Nationale Industrielle Aerospatiale v. United States Dist. Court for S. Dist.*, 482 U.S. 522, 544 n.29, 107 S. Ct. 2542, 96 L. Ed 2d 461 (1987); *see also Richmark Corp. v. Timber Falling Consultants*, 959 F.2d 1468, 1474 (9th Cir. 1992); *United States v. Vetco, Inc.*, 691 F.2d 1281, 1287 (9th Cir. 1981); May 29 Order 29:14-17. Assuming, *arguendo*, that Netherlands law would prohibit the discovery ordered, the Magistrate Judge analyzed the issue under the applicable legal standard, considered the relevant, non-exhaustive list of factors enumerated in *Richmark Corp.*, and determined that the factors

weighed in favor of permitting the ordered discovery. Although Defendants disagree with the Magistrate Judge's ultimate decision, they have failed to establish that her factual findings were clearly erroneous or that her legal conclusions were contrary to law.

VI. Defendants' Control of the Routing of Server Log Data

Defendants' final objection is a cryptic argument that the Magistrate Judge's factual finding that "Defendants have the ability to manipulate at will how the Server Log Data is routed" is clearly erroneous because it was based on insufficient evidence. In support of this contention, Defendants state that "Panther," the third-party service Defendants recently began using that prevents requests being received in the RAM of Defendants' servers, "never logged." However, as Defendants' representative testified during the Magistrate Judge's evidentiary hearing, Defendants "could disengage and resume the functions currently performed by Panther if directed to log the Server Log Data in issue." (May 29 Order 10:27-28 (citing RT 72, 103-04).)

The Magistrate Judge's factual findings were based on a full day of testimony, including testimony by expert witnesses called by both parties, as well as hundreds of pages of briefing, technical declarations, and even multiple rounds of supplemental briefing. Her finding that the "data in issue which is currently routed to a third party entity under contract to defendants and received in said entity's RAM . . . is within defendants' possession, custody or control by virtue of defendants' ability to manipulate at will how the data in issue is routed" was founded on her "consideration of the extensive arguments and evidence presented" and "the court's assessment of the credibility of the declarants and witnesses." (May 29 Order 1:25-2:8.) Moreover, the Magistrate Judge's decision with respect to Defendants' ability to route the Server Log Data to themselves or through Panther at will was also based on "the change in the method of operation" from routing the data to Defendants' servers to employing Panther

"and the timing thereof," as Defendants engaged Panthers' services just one month prior to the Magistrate Judge's evidentiary hearing. (*Id.* at 8:24-10:28.) As the record reflects that Defendants have the ability to reroute the Server Log Data through their own servers, should it prove impracticable for Defendants to acquire the information from Panther, the Court finds that the Magistrate Judge's finding that Defendants' control the routing of the Server Log Data was not clearly erroneous.

CONCLUSION

For the foregoing reasons, the Court hereby **DENIES** Defendants' Motion for Review (docket no. 194).

IT IS SO ORDERED.

Dated: August 24, 2007

FLORENCE-MARIE COOPER, JUDGE
UNITED STATES DISTRICT COURT