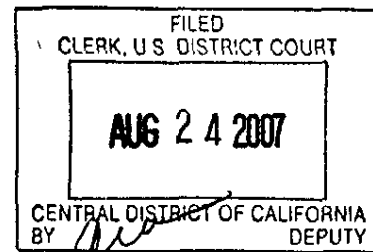
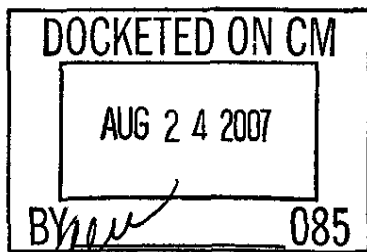


P Send



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.

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

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

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

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

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

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

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

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

21 ² Rule 34(a) states, in part, that “[a]ny party may serve on any other party a
 22 request . . . to produce and permit the party making the request, or someone
 23 acting on the requestor’s behalf, to inspect, copy, test, or sample *any* designated
 24 documents or *electronically stored information*--including writings, drawings,
 25 graphs, charts, photographs, sound recordings, images, and other data or data
 26 compilations stored *in any medium from which information can be*
 27 *obtained*--translated, if necessary, by the respondent into reasonably usable form,
 28 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).

1 clear evidence that Rule 34(a)'s scope was intended to be as broad as possible,
 2 and cover data stored "in any medium from which information can be obtained,"
 3 leaves no room to interpret the Rule to categorically exclude information written
 4 in a particular medium simply because that medium stores information only
 5 temporarily. Information in the RAM of Defendants' computers "can be
 6 obtained" by Defendant. It is undisputed that the Server Log Data³ Plaintiffs seek
 7 can be copied from RAM in Defendants' computers and produced to Plaintiffs.
 8 Rule 34 requires no greater degree of permanency from a medium than that
 9 which makes obtaining the data possible. As information can be obtained from
 10 RAM, it is within the scope of Rule 34 and subject to discovery under the
 11 appropriate circumstances.

12 Finally, as discussed in the Magistrate Judge's May 29 Order, *amici* and
 13 Defendants' argument that data in RAM is too ephemeral to satisfy Rule 34's
 14 storage requirement is foreclosed by the Ninth Circuit's decision in *Mai Systems*
 15 *Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993). To determine if the
 16 plaintiff could prevail on a claim of copyright infringement, the court in *Mai*
 17 *Systems Corp.* confronted the question of whether a program in RAM was "fixed
 18 in a tangible medium of expression," which the applicable statute defined as
 19 "sufficiently permanent or stable to permit it to be perceived, reproduced, or
 20 otherwise communicated for a period of more than transitory duration." *Id.* at
 21 517-518; 17 U.S.C. § 101. Despite the Copyright Act's explicit requirement that
 22 the medium store information with a degree of permanence and for "more than
 23 transitory duration," the court held that a computer's copying of software into

24
 25 ³ Server Log Data, as defined in the May 29 Order, includes (1) the
 26 anonymous (masked or encrypted) Internet Protocol (IP) address of users of
 27 Defendants' website who request dot-torrent files, (2) the identity of the dot-
 28 torrent files requested, and (3) the dates and times of such requests. (May 29
 Order, 3:16-4:1.)

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

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

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

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

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

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

7 Plaintiffs’ Motion to Require Defendants to Preserve and Produce Server
8 Log Data and for Evidentiary Sanctions was neither a motion for injunctive relief
9 nor its functional equivalent, and the May 29 Order granting the motion did not
10 dispose of any of Defendants’ claims or defenses. The May 29 Order is a
11 quotidian discovery order, resolving disputes over relevance, burden, and the
12 proper scope of discovery, that is well within the Magistrate Judge’s authority
13 and substantial specialized expertise. Magistrate judges regularly compel
14 production of documents and, although courts in other jurisdictions have
15 interpreted orders to preserve evidence as injunctions, the Ninth Circuit has held
16 that all parties are under a duty not to intentionally dispose of evidence they
17 know is relevant. *Idaho Potato Comm’n v. G&T Terminal Packaging, Inc.*, 425
18 F.3d 708, 720 (9th Cir. 2005); *Pueblo of Laguna v. United States*, 60 Fed. Cl.
19 133, 138 (2004) (holding that “a document preservation order is no more an
20 injunction than an order requiring a party to identify witnesses or to produce
21 documents in discovery.”) (citing *Mercer v. Magnant*, 40 F.3d 893, 896 (7th Cir.
22 1994); *cf. Madden v. Wyeth*, No. 3-03-CV-0167-R, 2003 U.S. Dist. LEXIS 6427,
23 at *1 (N.D. Tex. Apr. 16, 2003) (“A motion to preserve evidence is an injunctive
24 remedy and should issue only upon an adequate showing that equitable relief is
25 warranted.”).

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

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

10 **III. The Fifth Amendment**

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

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

1 intentionally exceed[ing] an authorization to access that facility; and thereby
2 obtain[ing] . . . authorized access to a wire or electronic communication while it
3 is in electronic storage in such system” The May 29 Order, however,
4 contemplates no *unauthorized* access. Defendants are not ordered to access the
5 facility of a third party and obtain stored communications, such as e-mails stored
6 on a remote server. Defendants are also not custodians of private
7 communications, as an Internet Service Provider would be of e-mails sent
8 through its servers (where neither the sender nor the recipient would be parties to
9 the litigation), ordered to disclose the contents of those communications. *Cf.*
10 *Theofel v. Farey-Jones*, 341 F.3d 978, 985 (9th Cir. 2003). Rather, Defendants
11 are the intended recipients of the information contained in the Server Log Data.
12 When users access Defendants’ website and request information (such as dot-
13 torrent files), they voluntarily supply their IP addresses and a packet of
14 information containing their request. That information is received and processed
15 in Defendants’ RAM on their servers, for their use (which, in addition to the
16 contemporaneous fulfillment of the request, the record reveals has thus far
17 consisted primarily of disclosure to advertisers to generate revenue). (May 29
18 Order 22:1-3; Reporter’s Transcript of the April 3, 2007, Discovery Hearing (RT)
19 90-97).) Defendants’ access to Defendants’ information on servers under
20 Defendants’ control does not constitute unauthorized access to a “facility through
21 which an electronic communication service is provided” or “to a wire or
22 electronic communication while it is in electronic storage in such system.”
23 Production of the Server Log Data would therefore not violate the SCA.

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

1 in electronic storage and actionable under the SCA, but not both. *Konop v.*
2 *Hawaiian Airlines, Inc.*, 302 F.3d 868, 877 (9th Cir.2002). As such, an electronic
3 communication may not simultaneously be actionable under both the Wiretap Act
4 and the SCA. *Id.* The Ninth Circuit has held that the Wiretap Act applies only to
5 “acquisition contemporaneous with transmission,” and that “Congress did not
6 intend for ‘intercept’ to apply to electronic communications when those
7 communications are in ‘electronic storage.’” *Theofel*, 359 F.3d at 1077-78,
8 quoting *Konop*. 302 F.3d at 877. Communications are in “electronic storage”
9 under the SCA, and outside the scope of the Wiretap Act, even where the storage
10 is transitory and lasts for only a few seconds. *Quon v. Arch Wireless Operating*
11 *Co.*, 445 F. Supp. 2d 1116, 1135-36 (C.D. Cal. 2006) (citing *Konop*, 302 F.3d at
12 878 n.6). As discussed above, the Server Log Data exists in electronic storage.
13 The Wiretap Act is therefore inapplicable and does not pose any barrier to
14 Defendants’ compliance with the May 29 Order.

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

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

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

10 For example, Defendants note that the Magistrate Judge concluded that
11 "preservation and production of the Server Log Data is appropriate in light of the
12 conclusory and speculative nature of the evidence presented regarding the loss of
13 good will and business, the key relevance and unique nature of the Server Log
14 Data in this action, the lack of a reasonable alternative means to obtain such data,
15 and the limitation imposed by the court regarding the masking of IP addresses."
16 Defendants argue they were not able to present evidence of "alternative means to
17 obtain such data" because "the evidence needed for such proof has been
18 concealed by Plaintiffs in an institutional citadel of privilege." (Mot. 41:1-2.)

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

26
27 ⁴ As the Court's holding rests on independent legal grounds, it is
28 unnecessary to review the Magistrate Judge's determination that Defendants'
website constitutes an "electronic communications service."

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

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

21 **IV. The First Amendment**

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

1 Server Log Data does not encroach or substantially encroach” upon the limited
2 First Amendment protection to which the users of Defendants’ website are
3 entitled, “particularly in light of the fact that such data does not identify the users
4 of Defendants’ website and that the IP addresses of such users have been ordered
5 to be masked.” (May 29 Order 23:3-7.)

6 Defendants argue that, under *Adolph Coors Co. v. Wallace*, 570 F. Supp.
7 202, 208 (N.D. Cal. 1983), the Magistrate Judge was required to employ a formal
8 three-part balancing test in determining whether to order the requested discovery.
9 *Adolph Coors Co.*, in addition to not constituting binding precedent, proposed
10 only that “any tribunal confronted with facts and arguments similar to those
11 presented here undertake a sensitive evaluation in three steps.” *Id.* In *Adolph*
12 *Coors Co.*, the defendant Solidarity was a political organization comprised
13 exclusively of gay men and lesbian women who sought to exert pressure on the
14 plaintiff brewing company through a boycott in an effort to modify the plaintiff’s
15 political positions. *Id.* at 204. The plaintiff requested a list of the names of
16 Solidarity’s members and its sources of financial support. *Id.* Solidarity argued
17 that revealing the group’s members and donors would chill its associational
18 privacy and freedom of political expression. *Id.*

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

1 (1985) (“The essential thrust of the First Amendment is to prohibit improper
2 restraints on the *voluntary* public expression of ideas; it shields the man who
3 wants to speak or publish when others wish him to be quiet. There is necessarily,
4 and within suitably defined areas, a concomitant freedom *not* to speak publicly,
5 one which serves the same ultimate end as freedom of speech in its affirmative
6 aspect.”) (emphasis in original) (internal quotations omitted)); *A&M Records v.*
7 *Napster, Inc.*, 239 F.3d 1004, 1028 (9th Cir. 2001) (holding that the First
8 Amendment does not protect use of a peer-to-peer file sharing network that
9 constitutes copyright infringement). Even if the users are engaged in *legal* file
10 sharing, they have little to no expectation of privacy because they are
11 broadcasting their identifying information to everyone in the BitTorrent “swarm”
12 as they download the file. *See, e.g., In re Verizon Internet Servs.*, 257 F. Supp. 2d
13 244, 267 (D.D.C. 2003) (finding that “if an individual subscriber opens his
14 computer to permit others, through peer-to-peer file-sharing, to download
15 materials from that computer, it is hard to understand just what privacy
16 expectation he or she has after essentially opening the computer to the world.”).
17 Similarly, because users openly disclose their IP addresses as part of the
18 BitTorrent file transfer process, the Court is not persuaded by Defendants’
19 argument that the retention of the IP addresses of users who obtain dot-torrent
20 files from Defendants’ website will “chill” their speech. Accordingly, the Court is
21 satisfied that the Magistrate Judge properly weighed Defendants’ First
22 Amendment concerns against the need for the requested discovery, and that her
23 resolution of the matter was not contrary to law.

24 **V. Impact of International Law**

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

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

8 A service provider may, in certain circumstances, be obliged to
9 provide rights holders (or their representatives) with the information
10 asked for. For this, the Court must first of all be satisfied that there
11 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.

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

18 Second, as the Supreme Court has stated, "[i]t is well settled that [foreign]
19 statutes do not deprive an American court of the power to order a party subject to
20 its jurisdiction to produce evidence even though the act of production may violate
21 that statute." *Societe Nationale Industrielle Aerospatiale v. United States Dist.*
22 *Court for S. Dist.*, 482 U.S. 522, 544 n.29, 107 S. Ct. 2542, 96 L. Ed 2d 461
23 (1987); see also *Richmark Corp. v. Timber Falling Consultants*, 959 F.2d 1468,
24 1474 (9th Cir. 1992); *United States v. Vetco, Inc.*, 691 F.2d 1281, 1287 (9th Cir.
25 1981); May 29 Order 29:14-17. Assuming, *arguendo*, that Netherlands law
26 would prohibit the discovery ordered, the Magistrate Judge analyzed the issue
27 under the applicable legal standard, considered the relevant, non-exhaustive list
28 of factors enumerated in *Richmark Corp.*, and determined that the factors

SCANNED

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

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

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

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

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

8 CONCLUSION

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

11
12
13 **IT IS SO ORDERED.**

14 Dated: August 24, 2007

15
16
17 
18 FLORENCE-MARIE COOPER, JUDGE
UNITED STATES DISTRICT COURT
19
20
21
22
23
24
25
26
27
28