Ira P. Rothken (SBN #160029)
Robert L. Kovsky (SBN #61770)
ROTHKEN LAW FIRM LLP
3 Hamilton Landing, Suite 280
Novato, CA 94949
Telephone: (415) 924-4250
Facsimile: (415) 924-2905

Kirk J. Retz (#170208)
Deann Flores Chase (#183937)
RETZ & HOPKINS, LLP
21535 Hawthorne Blvd., #200
Torrance, CA 90503
Telephone: (310) 540-9800
Facsimile: (310) 540-9881

Attorney for Defendants
Justin Bunnell, Forrest Parker, Wes Parker and Valence Media, Ltd.

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

COLUMBIA PICTURES INDUSTRIES, INC., et al.

Plaintiffs,

vs.

JUSTIN BUNNELL, et al.,

Defendants.

Case No. 06-01093 FMC

MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF DEFENDANTS' OBJECTIONS TO AND MOTION FOR REVIEW OF ORDER RE SERVER LOG DATA

DATE: July 16, 2007
TIME: 10:00 a.m.
CTRM: 750
Hon. Florence Marie Cooper

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

CASES

STATUTES

As set forth in the accompanying "Notice of Hearing on Defendants' Objections To and Motion for Review of Order Re Server Log Data and Objections to Such Order," (hereinafter "Defendants' Notice") and pursuant to 28 U.S.C. 636(b)(1), Federal Rule of Civil Procedure 72(a) and Local Rule 72-1, ***Defendants object to*** the "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 Attorney's Fees and Costs" of Magistrate Judge Jacqueline Chooljian (hereinafter "Magistrate Judge's Order" or "the Order") ***and move this Court to review the Magistrate Judge's Order***, to receive further evidence and to reconsider, set aside or modify the Order and/or recommit the matter to the Magistrate Judge. The Magistrate Judge's Order is attached to the Notice. The grounds stated in the Notice organize and summarize the Legal Argument set forth infra in this Memorandum of Points and Authorities.

I

INTRODUCTION

The Magistrate Judge's Order compels Defendants, operators of a website, to "preserve the Server Log Data for the duration of the this litigation." (Order at 33:16-17.) The "Server Log Data" demanded by Plaintiffs will include information personal to a website visitor. Such data has never existed at Defendants' website; but Defendants are ordered to collect it and to hand it over to Plaintiffs, albeit with a "mask" that seems destined to be stripped away. The Magistrate Judge's Order is unprecedented and damaging to online Free Speech and privacy and to free market values that support technological development. The Magistrate Judge is ordering Defendants to construct "Server Log Data" out of fragments of data that pass through Random Access Memory ("RAM") in Defendants' webs servers and to create the means to record, store, preserve and process the Server Log Data. All

computer data passes through RAM and the Magistrate Judge's Order amounts to taking control of a party's computers for the benefit of its adversary. The Magistrate's Order constitutes a mandatory injunction, issued without bond, that is beyond the jurisdiction of the office. The Magistrate Judge's Order compels Defendants to create documents solely for production to Plaintiffs and is contrary to this Court's Order in *Paramount Pictures Corp. v. ReplayTV* (C. D. Cal. 2002) CV 01-9358 FMC (Ex) (filed May 30, 2002) 2002 WL 32151632.

A chief component of Server Log Data is a list of IP addresses of visitors to Defendants' website. An IP address can be used to identify a person because it uniquely identifies a personal computer's connection to the Internet. Plaintiffs and the Motion Picture Association of America ("MPAA") which Plaintiffs control, are reportedly collecting IP addresses and Personally Identifying Information ("PII") of suspected infringers for litigation purposes. Although the Magistrate Judge's Order requires "masking" the IP addresses, any protection is illusory because the Order states: "defendants are not, ***at least at this juncture***, ordered to produce such IP addresses in an unmasked/unencrypted form." (Order at 33:24-34:3, emphasis added.) An IP address is joined in the Server Log Data with the name of a file that Plaintiffs may, in an appropriate case, allege is a signal of copyright infringement.

Plaintiffs allege that Defendants' website is used by visitors to locate a place in the "BitTorrent Network" through which to exchange infringing copies of Plaintiffs' movies and television programs. No copyrighted materials are posted or pass through Defendants' website. Defendants run a search engine and provide downloads in support of a technology that is used for promulgation of large-size files to large numbers of recipients; and that technology can be used by software developers, by video game creators — and by copyright infringers.

Defendants do not monitor or filter activity on their website which is built around automated facilities. Defendants have never recorded IP addresses and have

always been adamantly opposed to recording IP addresses. Recording IP addresses is a violation of visitors' privacy and of online anonymity protected by the Free Speech clause of the First Amendment to the United States Constitution. Defendants' business is to attract visitors; recording IP addresses or "tracking visitors" is contrary to Defendants' business purposes. Defendants have a stated policy of not tracking visitors. The Magistrate Judge overrode Defendants protests and the Order compels Defendants to act contrary to their interests and in violation of values of online Free Speech and privacy.

In issuing the Order, the Magistrate Judge made several major unprecedented and erroneous rulings that will, unless reviewed and corrected, determine the outcome of this action and shape electronic jurisprudence and Internet development for long into the future.

Disregarding Constitutional protection for online Free Speech and anonymous speech, in an unprecedented ruling, the Magistrate Judge ruled that compelling the recording of IP addresses, along with other information, and the preservation of that information for production to Plaintiffs "does not encroach or substantially encroach upon such protection." (Magistrate Judge's Order at 23:4-5.) Privacy protections were similarly brushed aside. The Magistrate Judge did not even purport to carry out a balancing test as called for by established authorities. A balancing test would have failed because Plaintiffs never showed any ***need*** for the Server Log Data. The Magistrate Judge's Order confuses ***relevance*** with ***need***. Defendants are informed and believe that Plaintiffs have all the evidence they need, but that such evidence is concealed in a citadel of privilege that Plaintiffs have constructed within the MPAA. Plaintiffs refuse to respond to discovery attempts about such evidence but they also fail to affirmatively declare that they ***need*** the evidence. This Article III Court should make an independent determination of such Constitutional matters.

In another unprecedented ruling, the Magistrate Judge's Order compels Defendants to collect, record and preserve Server Log Data for all visitors, including the majority of the visitors who reside in countries other than the United States (and whose actions are not subject to United States courts) and visitors who have no connection whatsoever with any copyright infringement. Defendants' web servers, where the Magistrate Judge's Order must be carried out, are in the Netherlands and the law of the Netherlands, although not yet fully interpreted, appears to criminalize what the Magistrate Judge's Order compels to be done. The chief reason given by the Magistrate Judge for disregarding the law of the Netherlands is "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." (Magistrate Judge's Order at 30:9-12.) In other words, Defendants are to be punished for seeking privacy protections in the Netherlands, a lawful free choice, by having those protections stripped away, not only from Defendants but from their visitors as well, even citizens of the Netherlands. This Court should review the Magistrate Judge's Order.

The Magistrate Judge's Order also disregards the Electronic Communications Privacy Act (ECPA) and the Pen Register Statute. In violation of the most basic due process safeguards, the Magistrate Judge ruled that Defendants had "consented" to the Magistrate Judge's Order, as if Defendants' consistent opposition to the compulsory Order was not even worth noticing. The Magistrate Judge misread 18 U.S.C. § 2702 (Magistrate Judge's Order at 23:17), which is titled "Voluntary disclosure of customer communications or records" and this Court should review the Order.

The most serious jurisprudential error was the Magistrate Judge's determination that the existence of pieces of data in RAM was equivalent to the

existence of "electronically stored information," a category added to the 2006 Amendments to Federal Rule of Civil Procedure 34. Using self-validating circular reasoning, the Magistrate Judge made a maximal and conclusive determination that forecloses any future refinement and that is contrary to the approach of the Advisory Committee that calls for more sensitivity to the difficulties of crafting developing law so as not to cripple technology. All computer data passes through RAM. There is no compact unity or functional integrity to data just because it passes through RAM and there is none here. Any unity or integrity imposed upon the data passing through RAM will be the result of Defendants' compliance with the Magistrate Judge's Order.

The Magistrate Judge's Order will subject a party in a technology case to demands from adversaries that the party's computers be turned into document creation, preservation and production systems for the benefit of the adversaries. Here, Plaintiffs demand that the top priority of Defendants' business must become the collection, recording, storage, preservation and processing of Server Log Data and the production of such data to Plaintiffs. To satisfy this demand, the Magistrate Judge is taking control of Defendants' business and making it serve the will of Plaintiffs, under an unsupportable finding that "Defendants Have the Ability to Manipulate at Will How the Server Log Data is Routed" (Order at 10:25-26 and 15:9-10; see also 29:4-5.) The Order is a mandatory injunction, issued without bond, in excess of the Magistrate Judge's jurisdiction under 28 U.S.C. 636(b)(1)(A) ("except a motion for injunction").

To carry out the Magistrate Judge's Order, Defendants will be compelled to create new documents solely for their production to Plaintiffs, contrary to this Court's rulings in *Paramount Pictures Corp. v. ReplayTV* (C. D. Cal. 2002) CV 01-9358 FMC (Ex) (filed May 30, 2002) 2002 WL 32151632. Throughout, Defendants have relied on those rulings. Those rulings show a simple, practical

way to resolve this dispute. Because The Magistrate Judge's Order compels Defendants to create documents solely for production to Plaintiffs, it should be reviewed, set aside or modified. In the alternative, the Court should receive further evidence or recommit the matter to the Magistrate Judge.

II.
FACTUAL BACKGROUND

Defendants operate a website, "Torrentspy," located on the World Wide Web at www.torrentspy.com, that chiefly hosts a search engine. Defendants' website incorporates automated processes that search the Internet for "dot-torrent" files, which end in ".torrent" the way Adobe Acrobat files end in ".pdf." A dot-torrent file is a component of BitTorrent technology, described below, that is widely used for online promulgation of large files such as software updates and video games. Defendants' automated processes collect and organize dot-torrent files and typically download them to users who enter requests through Defendants' search engine.

Torrentspy is among the top 200 websites in the world measured by the volume of traffic. (Transcript of Proceedings of April 3, 2007 (hereinafter "Tr.") at 102:17-21, Exhibit V to the accompanying Declaration of Ira P. Rothken.) Approximately 70% of Torrentspy's traffic originates in countries other than the United States. (Tr. at 103:5-11; 117:23 - 118:4.) Torrentspy's web servers are maintained by a third-party provider, Leaseweb, at a secure plant in Amsterdam, the Netherlands. (See Magistrate Judge's Order at 28:4-7.)

Plaintiffs allege that visitors to Defendants' website use dot-torrent files found there to exchange files containing unauthorized versions of their copyrighted movies and television programs. Defendants acknowledge the likelihood that some visitors use Defendants' search engine for such infringing purposes. No infringing materials are posted on Defendants' website and any infringement occurs without

involvement of Defendants' website other than provision of a dot-torrent file. The automated processes aggregate dot-torrent files found by searching the Internet and there is no monitoring or filtering. Dot-torrent files are devoid of copyrighted material.

Torrentspy can be used by good people and by bad people. Google is no different and both have much the same database as far as dot-torrent files are concerned. Defendants provide services to their customers without policing their customers and that is the nature of their competitive business. Defendants have neither a unique nor an essential position in the BitTorrent community. Major competitors are overseas, beyond the reach of U.S. courts.

Defendants' business plan is that their system is free and attractive to users who view it, use its search engine, download dot-torrent files and visit the advertisers. The website declares that personal information is not being collected without a person's consent. As part of their business plan, defendants decided not to collect what Plaintiffs call "Server Log Data" because of their "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 reasons" (See Magistrate Judge's Order at 7:18-8:1 and footnote 10 at 8:13-23.)

The Magistrate Judge's Order compels Defendants to collect, record, store, preserve, process and produce such "Server Log Data", namely:

> "(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." (Magistrate Judge's Order at 3:15-4:1.)

Under the Magistrate Judge's Order, the items of data must be picked out or selected item by item from streams of data that pass through the servers at Defendants' website and then organized into records. The undisputed evidence establishes that Defendants have never selected, recorded or preserved data in such

a form, have never recorded or preserved IP addresses of users in any form, and have always been opposed, on privacy grounds, to recording IP addresses. (Magistrate Judge's Order at 7:5-8:5.) The daily volume of data that must be preserved is so large as to require either new hardware installations or new arrangements with Leaseweb in the Netherlands or some other new arrangement. (See Magistrate Judge's Order at 19:7-15.) The Magistrate Judge's Order also requires Defendants to discontinue an existing beneficial contract with a third-party provider, Panther, whose services to Defendants interfere with the Order. (See Judge Magistrate's Order at footnote 14, 11:21-28 and 12:17-28.)

During the hearing before the Magistrate Judge, Defendants tried to show the impracticalities of Plaintiffs' various proposals for handling Server Log Data, but the Magistrate Judge disregarded and rejected the core of Defendants' evidence.

The Magistrate Judge's Order does not specify how Defendants are to carry out its commands but rather states:

> "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." (Magistrate Judge's Order at 33:18-20.)

The Magistrate Judge's Order further orders Defendants "to mask users' IP addresses before the Server Log Data is produced." (Magistrate Judge's Order at 21:8-9.)

> "Although defendants are required to preserve the IP addresses of the computer used to request dot-torrent files, defendants are not, ***at least at this juncture***, ordered to produce such IP addresses in an unmasked/unencrypted form. Instead, defendants shall mask, encrypt, or redact IP addresses through a hashing program or other means, provided, however, that if a given IP address appears more than once, such IP address

is concealed in a manner which permits one to discern that the same IP address appears on multiple occasions." (Magistrate Judge's Order at 33:24-34:7, emphasis added.)

As we understand the Magistrate Judge's Order, it requires Defendants to perform a series of tasks:

(1) to collect the Server Log Data from streams of data passing through Defendants' servers, in effect ordering Defendants to either "turn on" the generic server logging function in the Microsoft IIS system that runs the website servers or to write their own "programmatic method." (See Magistrate Judge's Order at 18:19-23);

(2) to record the Server Log Data in a file (a major point of controversy because of disputes over the size of the file generated);

(3) to store the Server Log Data in a permanent form (up to this point, all such data has been transient);

(4) to preserve the Server Log Data (implicitly involving a chain of custody e.g., from Amsterdam to Defendants' offices in California);

(5) to process the Server Log Data (masking the IP addresses); and

(6) to produce the Server Log Data to Plaintiffs.

Defendants also anticipate that they and anyone who is involved with the Server Log Data must be ready (7) to defend the truth and integrity of that data in adversarial proceedings, e.g., during a testimonial contest with Plaintiffs' retained expert witnesses. (See Magistrate Judge's Order at 5:22-28.)

Defendants contend, as their leading point, that the Magistrate Judge's Order awards to Plaintiffs the essence of the injunctive relief Plaintiffs are seeking in their Complaint and that the Magistrate Judge acted in excess of her statutory jurisdiction under 28 U.S.C. § 636(b)(1)(A) ("except a motion for injunctive relief"). In brief, in their Complaint Plaintiffs are asking the Court to control details of Defendants'

website operations and the ways Defendants deal with their visitors. Plaintiffs want Defendants ordered to assume the duties of involuntary and unpaid guardians of plaintiffs' copyrights by being required to filter dot-torrent files available through the website to exclude infringing materials, with a contempt citation threatened for any shortfall in perceived performance.

Now, through a discovery order, Plaintiffs have achieved the purposes of their principal action, with a contempt citation in the offing if Defendants fail to meet Plaintiffs' demands for Server Log Data. Defendants' protests against being compelled to record IP addresses and other data are ignored, Defendants' privacy policy is overridden, Defendants' DMCA policy and affirmative defenses are ignored, and Defendants' evidence of impracticalities is disregarded. Defendants are ordered to perform immediately tasks that they say are difficult and burdensome, if not impossible, because plaintiffs' expert witness, Ellis Horowitz, testified that they are easily done and because the Magistrate Judge disbelieved Defendants and dismissed their testimony. (Magistrate Judge's Order at 5:22-28,

17:23 and 18:10-21:2.)[1]

Should, through extraordinary efforts, Defendants succeed in performing the tasks imposed on them by the Magistrate Judge and create and deliver to Plaintiffs the Server Log Data that Plaintiffs demand, Plaintiffs will use that success to argue about how easily Defendants could take on duties of guarding Plaintiffs' copyrights from infringement and how nothing Defendants say about difficulties needs to be taken seriously. Defendants' Free Speech and privacy concerns, for example, will be unimportant because the Court will have already gone almost the whole way in the invasions Plaintiffs are seeking and any additional invasion will be slight in comparison. The Magistrate Judge has decided against Free Speech and privacy rights in her Order and that decision will have become final as a matter of fact.

The allegations of the Complaint and undisputed facts show how Plaintiffs will have accomplished their final goals through issuance of the Magistrate Judge's

---

[1] One controversy was whether Defendants' could filter the data at the point of origin according to criteria that would selectively log data, thus reducing the resulting volume. "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)." (Magistrate Judge's Order at 19:18-22.) In the referenced portion of the transcript, Plaintiffs' counsel handed a document to Defendant Parker on the witness stand that counsel represented had been downloaded from a Microsoft support website. Defendant Parker testified that he had never seen the document before. Counsel asked "Does that in any way refresh your recollection that the web server IIS can create server logs for limited amounts of data, specifically data to a particular folder" and Defendant Parker answered "It looks like it." This testimony does not prove any pertinent point and is unrelated to the rest of Defendants' evidence. Even supposing that Parker was in error on this matter, such an error was not a proper basis to discredit all of Parker's testimony of first-hand experience with Defendants' system. (*Id*., at 20:18-19.)

Order unless that Order is reviewed and set aside or modified by this Court.

Dot-torrent files are one component needed to transfer files using BitTorrent technology. "BitTorrent is a peer-to-peer network optimized for the copying and distribution of large files. On a 'peer-to-peer network, the actual exchange of the files — *i.e.*, the actual downloading and uploading — takes place directly between users (or 'peers') of the network." (Complaint, Exhibit A to the accompanying Rothken declaration at 3:26-4:2.)

BitTorrent technology is used by software developers like Linux, video-game creators and other technology companies to promulgate updated versions of large-scale computer files. In BitTorrent technology, every person who downloads from a source then becomes a source for other persons. The demands on computers needed to carry out the transfers are ***distributed***: instead of a central server that must send the same file million of times to millions of recipients, a few "seeders" start the promulgation and each recipient sends the contents on to others, ultimately to anyone wanting it who is connected to the Internet. In Internet parlance, the seeder attracts a ***swarm*** of users who exchange copies among themselves. (Because a large-sized work is promulgated in pieces, users are trading pieces.)

The advantages to Plaintiffs and to other producers of large-sized digital works are obvious. What is now in a DVD can be sold and delivered to tens of millions of consumers with essentially zero costs to the producers for media production or distribution.

Unfortunately for Plaintiffs, thousands of individuals are ripping open the security system of present-day Digital Video Discs (DVDs) containing Plaintiffs' copyrighted movies and television programs, extracting the contents and transferring infringing copies through BitTorrent technology to hundreds of thousands of recipients that gather in swarms for the purpose of obtaining them "free." There is no central focus of activity (as in the *Napster* and *Grokster* cases);

rather all activity is distributed. As a matter of fact, closing down Defendants will have little if any direct effect on copyright infringement because Defendants have many competitors. Defendants are only a representative company that services one sector of the BitTorrent community, a community made up of the many persons residing all over the world who are using BitTorrent technology to exchange files. (Complaint at ¶¶ 10, 12-14.) Plaintiffs are indifferent to Torrentspy. Plaintiffs want a scapegoat whose sacrifice will erode online Free Speech and privacy protections as part of an ongoing campaign against "piracy." Plaintiffs want to warn off Internet businesses from developing resources that infringers might use.

Apparently, Plaintiffs, the MPAA and other copyright owners envision a future for the Internet that they believe will satisfy their needs. The owners will themselves promulgate their copyrighted works using BitTorrent technology, but with a built-in Digital Rights Management ("DRM") system that will enable them to control the uses of the materials. Promulgation will be through Internet companies that either partner with the owners or that comply with the owners' requirements. (E.g., Plaintiff Warner Bros. signed a highly-publicized contract with bittorrent.com.) Such companies will be required to exclude any materials that offend the owners through copyright infringement or otherwise. The owners will use litigation to shut down independent companies, like Defendants' company, that maintain resources for the promulgation of materials that offend the owners. To the extent the Internet remains open to independent providers, copyright infringers will make use of their resources, justifying the owners' litigation program. The owners envision that their friends, the "legitimate" BitTorrent companies, will flourish while they police the Internet, using the Courts to punish offenders. Those whose offense is independence will be punished in the name of copyright protection. The case against Torrentspy is to be a paradigm that will support future development.

Plaintiffs' vision is unrealistic because the Internet is global and because

Plaintiffs' reach does not extend beyond the jurisdiction of the United States. Plaintiffs cannot control or shut down a company that has no ties to the United States. Plaintiffs' vision is also unrealistic because it is a static vision that cannot adapt to changes in technology or to the creative wiles of the "pirates." All that Plaintiffs can accomplish is to stifle development in the United States of BitTorrent technology and other technologies that might be used by copyright infringers.

Plaintiffs' vision is contrary to principles stated by the United States Supreme Court in favor of Free Speech and open Internet development.[2] In such cases, Congress sought to protect children from online indecency and other harmful materials, but two Attorneys General failed to persuade the Court that the constraints could be imposed in the face of the First Amendment. Rather, it was held that online Free Speech and Internet development are values of greater weight than protecting children from online indecency and harmful materials. Now, this Court must weigh Free Speech, privacy and Internet development, as well as Defendants' right to carry on their business, against the rights of copyright owners.

Large-scale and ultimate features of this case are reproduced on the smaller stage of this Motion. The essence of the relief Plaintiffs are seeking through their Complaint is granted in the Magistrate Judge's Order.

In particular, Plaintiffs are alleged to be secondarily liable for copyright infringement because visitors use Defendants' search engine to locate "dot-torrent" files that are popular among file exchangers, including dot-torrent files with names

---

[2] The Internet provides "the most participatory form of mass speech yet developed," *ACLU v. Reno*, 929 F. Supp. 824 (E.D. Pa. 1996) at 883, upheld in *Reno v. ACLU*, 521 U.S. 844, 870, 138 L. Ed. 2d 874, 117 S. Ct. 2329 (1997). See also *Ashcroft v. Free Speech Coalition*, 535 U.S. 234, 122 S. Ct. 1389; 152 L. Ed. 2d 403 (2002); *Ashcroft v. ACLU*, 542 U.S. 656, 673, 124 S. Ct. 2783, 159 L. Ed. 2d 690 (2004) (burden of filtering Internet content for materials harmful to children should be borne by parents rather than by constraining general Internet activity).

that correspond to Plaintiffs' copyrighted works. (Complaint, ¶¶ 9, 12, 27-28.) "Defendants index [dot-]torrent files of television programs by *the titles of individual copyrighted television series*, including 'Alias' and 'The Simpsons.'" (Complaint at 8:4-5, emphasis in original.) "Defendants easily could prevent infringement of Plaintiffs' copyrighted works by not indexing [dot-]torrent files corresponding to Plaintiffs' copyrighted works. ***Defendants also have the ability to decide which users can access their torrent site***, including the right and ability to exclude or ban specific users, such as by not allowing users with particular login names to upload or download torrent files." (Complaint at 8:20-25, emphasis added.) Plaintiffs seek injunctive relief, using the broadest possible language. (Complaint at 11:21-12:5.)

Plaintiffs demand that Defendants use their "ability" to "exclude or ban specific users." Because visitors to Defendants' websites are presently anonymous, Plaintiffs' claims for relief incorporate a demand that Defendants track users and their activities by recording, storing, and processing a user's IP addresses and the dot-torrent files a user accesses. This is exactly what the Magistrate Judge's Order now compels. The systems needed to preserve Log Server Data will be adapted to "exclude or ban specific users" and to satisfy the demand that Defendants exclude dot-torrent files on the basis of an appearance of a word like "alias" or a name like "Simpson." Indeed, the Magistrate Judge's Order will be the core of any final injunctive relief that is hereafter Ordered.

The main factual finding that Defendants challenge here is the comprehensive finding that supports the command of the Magistrate Judge that Defendants must "find a way" to comply with the Magistrate Judge's Order. That is the general factual finding that "defendants have the ability to manipulate at will how the Server Log Data is routed" (Magistrate Judge's Order at 10:25-26 and 15:9-10.) The Magistrate Judge generalized from one specific manipulations to some

indefinitely large class of manipulations that could be carried out at the will of the Magistrate Judge or as set forth in the Final Decree. There is no basis in the record for such a generalization. With such a finding, the class of manipulations that the Magistrate Judge or the Final Decree can order is unconstrained by difficulties, costs, losses or other burdens and consequences. If the Magistrate Judge's finding is affirmed, Defendants will have become lackeys; and any independent will of their own will have vanished. Those who will control their business appear, at best, indifferent about its welfare, and it is likely doomed.

II

LEGAL ARGUMENT

A. The Magistrate Judge Did Not Have Authority or Jurisdiction to Issue the Discovery Order Because It Amounts to an Injunction That Disposes of Ultimate Issues in the Case.

Defendants submit that the Magistrate Judge's Order amounts to a mandatory injunction, issued without a bond. Issuance of the Order in excess of the authority allowable under 28 U.S.C. § 636(b)(1)(A) ("except a motion for injunctive relief") and is, therefore, "contrary to law" under Federal Rule of Civil Procedure 72(a).

In *Gomez v. United States*, 490 U.S. 858, 871-872, 109 S. Ct. 2237, 104 L. Ed. 2d 923 (1989), the Court reviewed the jurisdiction of magistrate judges and held that magistrates did not have the power to preside over jury selections at felony trials.

> "Through gradual congressional enlargement of magistrates' jurisdiction, the Federal Magistrates Act now expressly authorizes magistrates to preside at jury trials of all civil disputes and criminal misdemeanors, subject to special assignment, consent of the parties, and judicial review. The Act further details magistrates' functions regarding pretrial and post-

> trial matters, specifying two levels of review depending on the scope and significance of the magistrate's decision. The district court retains the power to assign to magistrates unspecified 'additional duties,' subject only to conditions or review that the court may choose to impose. By a literal reading this additional duties clause would permit magistrates to conduct felony trials. But the carefully defined grant of authority to conduct trials of civil matters and of minor criminal cases should be construed as an implicit withholding of the authority to preside at a felony trial. The legislative history, with its repeated statements that magistrates should handle subsidiary matters to enable district judges to concentrate on trying cases, and ***its assurances that magistrates' adjudicatory jurisdiction had been circumscribed in the interests of policy as well as constitutional constraints***, confirms this inference. Similar considerations lead us to conclude that Congress also did not contemplate inclusion of jury selection in felony trials among a magistrate's additional duties." (Emphasis added, footnotes omitted.)

In *Reynaga v. Cammisa*, 971 F.2d 414, 417 (9th Cir. 1992), the magistrate judge ordered a prisoner's pro se action stayed until the prisoner had exhausted his state remedies. The order "was beyond the magistrate's authority: it was beyond his jurisdiction and was, in essence, a legal nullity." Among other flaws in the stay order was its violation of "Subsection (1)(A) [which] specifically exempts 'motions for injunctive relief' from the category of pretrial matters upon which a magistrate may enter an order."

In *United States v. Rivera-Guerrero*, 377 F.3d 1064 (9th Cir. 2004), the Magistrate Judge ordered that medication be administered to a defendant against his will, for the purpose of making defendant competent to stand trial. The District Court denied defendant's motion to reconsider the magistrate judge's decision but

the Court of Appeals reversed. The Court based its analysis on *Sell v. United States*, 539 U.S. 166, 156 L. Ed. 2d 197, 123 S. Ct. 2174 (2003) and upon a dispositive/non-dispositive distinction implicit in the division of 28 U.S.C. § 636(b)(1)(A) (non-dispositive) and § 636(b)(1)(B) ("disposition by a judge").

> "The district court erred when it concluded that the involuntary medication order was not a final order and was therefore not dispositive. The court based its analysis of the non-dispositive nature of the order on the *Sell* Court's statement that an order to forcibly medicate 'is completely separate from the merits of the action.' *Sell*, 539 U.S. at 176 (internal quotation marks omitted). This analysis conflates the meaning of 'final' in two very different contexts: final as opposed to collateral and final as opposed to non-dispositive. ***It is quite conceivable that an order could not be 'final' due to its collateral nature and yet still be 'final' in the sense of its dispositive nature.*** In fact, that was precisely the situation in *Sell*. It was because the order was both collateral and dispositive that the Court found that it was appealable under the 'collateral order' exception. To fall under this exception, an order must 'conclusively determine the disputed question' -- in other words, it must be dispositive. *Id*. (alteration and internal quotation marks omitted). The *Sell* Court found that the involuntary medication order fulfilled this requirement. *Id*. ('The order . . . conclusively determines the disputed question, namely, whether Sell has a legal right to avoid forced medication.') (internal quotation marks omitted).
>
> "Furthermore, this disputed question is properly considered 'a claim or defense of a party.' [Citation.] ***The decision whether to issue an order authorizing involuntary medication will have direct consequences on Rivera's defense that he is not competent to stand trial.*** [Citation.] ***In***

addition, the order will be dispositive with regard to Rivera's affirmative claim that he has a constitutional right to be free from unwanted medication. While this claim is not directly tied to the merits of Rivera's case, it has crucial implications for his right to a fair trial. [Citation.]." 377 F.3d at 1078-1079 (emphasis added).

In *Vogel v. United States Office Prods. Co.*, 258 F.3d 509, 514-515 (6th Cir. 2001), the court stated that, to ascertain whether a motion was dispositive and therefore outside the authority of the Magistrate Judge, it would undertake "a functional analysis of the motion's potential effect on litigation."

Here, as in *Rivera-Guerrero*, the Magistrate Judge's Order has "direct consequences" on Plaintiffs' claims and Defendants' defenses, especially the First Amendment defense. Applying a "functional analysis" (*Vogel*), the Magistrate Judge's Order is essentially injunctive — compelling Defendants to operate their business in ways specified by Plaintiffs contrary to Defendants' prior operations and over Defendants protests. The Magistrate's commands go the merits of the case valuing plaintiffs' claims over online Free Speech and privacy, the ECPA and established procedures for dealing with copyright infringement set forth in the Digital Millennium Copyright Act ("DMCA"). Plaintiffs, through the Magistrate Judge's Order, are controlling detailed operations of Defendants' website involving visitors' identities and visitors' choices. Defendants are compelled to bear all the losses, burdens, costs and damages arising from the Order and there is no bond to compensate them if they lose site traffic and revenue from the Order and ultimately prevail on the merits of the case.

In their Answer, Defendants allege that the First Amendment to the United States Constitution and California's Privacy Amendment bar Plaintiffs' from taking over control of such detailed operations of Defendants' websites and protect the anonymity of visitors to Defendants' website. As a matter of fact, those issues have

now been resolved, by ordering Defendants to record IP addresses of visitors, despite Defendants' protests, through what appears to be a conclusion of law in the Order that its mandates are nothing more than an "insubstantial" encroachment on First Amendment protections.[3]

In *Sell*, as quoted in *Rivera-Guerrero*, supra, the issue was "whether Sell has a legal right to avoid forced medication." Here the issue is whether Defendants have a legal right to avoid forced website operations. Those legal right are put into issue by Plaintiffs' Complaint.

The Server Log Data Defendants are being compelled to collect, etc. is generated during the activities described in paragraphs 9 of the Complaint, and succeeding paragraphs. In paragraph 29 of the Complaint, Plaintiffs allege that "Defendants could easily prevent infringement of Plaintiffs' copyrighted works by not indexing torrent files corresponding to Plaintiffs' copyrighted works. Defendants also have the ability to decide which users can access their torrent site, including the right and ability to exclude or ban specific users." Using the broadest

---

[3] The Magistrate Judge's Order addresses such issues at 21:3-23:7. The Magistrate Judge found that "the users of defendants' website are entitled to limited First Amendment protection" but that "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." (*Id*., at 23:2-7.) Defendants submit that masking IP addresses is an illusory protection because the Magistrate Judge's states that "defendants are not, ***at least at this juncture***, ordered to produce such IP addresses in an unmasked/unencrypted form." (Magistrate Judge's Order at 34:2-3, emphasis added.) Plainly, the Court invites Plaintiffs to revisit masking. Masking is an important feature of the Magistrate Judge's Order. If IP addresses are masked, they provide no useful information; but if IP addresses are unmasked, the invasions of privacy are inflicted on all who visit Defendants' website, including visitors with entirely innocent purposes and visitors from all countries.

possible language, Plaintiffs seek injunctive relief that prohibits Defendants from "aiding, encouraging, enabling, inducing, causing, materially contributing to, or otherwise facilitating" unauthorized exchanges of copies of plaintiffs' copyrighted works. (Complaint at 11:25-26.) As their ultimate relief, Plaintiffs want the Court control "indexing torrent files corresponding to Plaintiffs' copyrighted works" on Defendants' website and to have the Court "decide which users can access their torrent site." They have achieved the greater part of those aims through the Magistrate Judge's Order.

The full effect of the Magistrate Judge's Order cannot be ascertained because the Order declines to specify ways that the Server Log Data must be collected, recorded, stored, preserved, processed and produced to Plaintiffs. To show the consequences of the Magistrate Judge's Order, we first set forth all its mandates:

> "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..." (Order at 33:15-17.)
>
> "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." (Order at 33:18-20.)
>
> "Defendants shall initially produce the Server Log Data [] by no later than two weeks from the date of this order. (Order at 33:21-22.)

The Magistrate Judge's Order further "directs defendants to mask users' IP addresses before the Server Log Data is produced." (Order at 21:8-9.) Specifications of the masking ordered by the Court are set forth at 33:24-34:7 of the Order.

In proceedings before the Magistrate Judge, Defendants protested that, if they were compelled to record IP addresses contrary to their longstanding public policies

and in face of their principled opposition to such recording, they also felt compelled to notify their visitors of the changes and to notify visitors of logging of IP addresses and of the circumstances of the logging. Defendants declared that the results might be disastrous for their business. Magistrate Judge's Order states:

> "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." (Order at 34:9-12.)

As Defendants understand the Magistrate Judge's Order, Defendants are put to the task of producing results in compliance with the Orders of the Magistrate Judge by whatever means Defendants can devise. Despite Defendants declarations of inability to comply, Defendants are ordered to find or even to invent means of compliance if necessary. If there any losses, those losses will be deemed the results of choices made by the Defendants. Defendants must bear all the consequences of compliance. And Defendants must comply, or they will be found in contempt.

Regardless of the possibility or impossibility of these commands, they plainly amount to a mandatory injunction. They also go to the merits of the litigation,

To show how thoroughly the Discovery Order pre-judges the case, Defendants consider possible, specific ways to comply. The situation cannot be fairly examined while "the methods" of compliance are completely unspecified and with all the risks of ambiguity thrown onto Defendants.

One major requirement of any means of compliance is that it withstand the closest possible scrutiny by Plaintiffs. Anyone involved in collecting, recording, storing, preserving, processing or producing the Server Log Data must expect to be questioned under oath by Plaintiffs' attorneys in discovery proceedings and must be prepared to engage in a testimonial contest with plaintiffs' expert witnesses. For

example, security of the data must be maintained at each step between initial collection and delivery to Plaintiffs. Someone has to testify that the data is true and correct. Forensic resources and skills must be incorporated in any compliance method. As the record reflects, Defendants risk being pilloried for any mis-statement, however innocent, were they to undertake the duties themselves. The means must be adapted to the sole purpose of the Server Log Data, namely, production to Plaintiffs and presentation in judicial proceedings.

We suppose that online forensics companies exist with the necessary resources and skills that can, for a price and with sufficient time, provide the services that will be in compliance with the Magistrate Judge's Order. There are difficulties arising from the high volume of data, the worldwide attraction of Defendants' website and imposed by the location of Defendants web server facilities in Amsterdam, the Netherlands; but we suppose that, with sufficient time and investment, these difficulties can be overcome. By putting the responsibilities into the hands of a third party, Defendants will have insulation, at least facially, from attacks on the data and directed at its keepers.

Hence, employment of such an online forensics company might satisfy the obligations of the Magistrate Judge's Order while providing some benefit to Defendants, if an online forensics company can be located that will undertake such services and if Defendants can survive in a competitive environment with the added costs and demands on its computer resources and burdened by an inability to adapt to the marketplace because of the rigid arrangements needed to create and produce Server Log Data. Creating Server Log Data in a trustworthy manner and producing that data to Plaintiffs will have become the overriding priority of Defendants' business.

Defendants submit that their employment of such an online forensics company and the means of compliance developed and put into operation by the online

forensics company will conclude chief issues in the principal litigation, namely, establishing the technical means for Defendants to comply with any ultimate Order of the Court and setting the terms for that ultimate Order. In defining a norm, nothing succeeds like success and there is no standard better than a standard that actually exists. The technical means established when Defendants comply with the Magistrate Judge's Order will become a floor for the ultimate Order of this Court and a platform for Plaintiffs' further demands. Defendants will have been compelled to establish those technical means under threat of a contempt citation with every step subject to examination by Plaintiffs' counsel; and those technical means will be tried and sure. The enforcement system will be in place and the enforcement order will be written for enforcement by that system.

The rejoinder, of course, is "Defendants chose to hire the online forensics company as means of complying with the Magistrate Judge's Order and Defendants chose a means that facilitates the Final Decree." Must Defendants comply with the Magistrate Judge's Order by a means that preserves the jurisdiction of the Magistrate Judge or to be deemed to waive any objection? And if Defendants testify that there was no other way to comply the Magistrate Judge's Order, does that not imply *a fortiori* that the technical means actually established by compliance with the Magistrate Judge's Order ***must*** be imposed through the Final Decree?

Or, perhaps, to avoid having an online forensics company prepare the means for their destruction, Defendants make a new arrangement with their overseas provider, Leaseweb, that maintains Defendants' web servers in Amsterdam. New equipment can be installed that will record the Server Log Data on tangible media that a service provider can pick up and replenish, also shipping the recorded media to Defendants in California for processing. In making such an arrangement, Defendants will employ such providers solely for the purpose of complying with the Magistrate Judge's Order. As a matter of commercial fair dealing, Defendants

must disclose to such providers that the new arrangement will be used to help Defendants to comply with that Order and that such providers might be subject to examination by Plaintiffs. We cannot predict the response of Leaseweb personnel to the Magistrate Judge's Order but anticipate that difficulties will be raised as to issues of local Dutch law, international law and privacy. Under the Magistrate Judge's Order, Defendants must clear up such issues. Compliance with the Magistrate Judge's Order will demonstrate, as a practical matter and, indeed, as a matter of principle, that issues of Dutch law, international law and privacy require little respect or consideration. Defendants will have been compelled, under threat of contempt, to establish the practices and principles that negate their defenses of privacy and international law.

No ambiguities as to means of compliance can conceal the hard truth that the Magistrate Judge's Order is a mandatory injunction without a bond, ordering Defendants to undertake duties of collecting, recording, storing, preserving, processing and producing to Plaintiffs new evidence through a means yet to be devised. The Magistrate Judge's command that Defendants create the means of compliance aggravates rather than lessens the injunctive nature of the Order. The Order commands Defendants to find the tools to dig their own grave and to prepare the plot. Under such circumstances, execution is fore-ordained. Such an Order is beyond the jurisdiction or authority of the Magistrate Judge and should be modified or set aside by this Court pursuant to Federal Rule of Civil Procedure 72(a).

B. The Magistrate Judge's Order Should Be Reviewed Because It Infringes on Constitutional Rights and Is Contrary to Law.

1. Because of the Constitutional Implications, an Article III Court Should Exercise Independent Judgment and Review the Magistrate Judge's Order.

In *Rivera-Guerrero*, supra, at 377 F.3d 1069-1070, dealing with involuntary administration of medicine, the Court discussed the principle (based on *Gomez*, supra) of "Constitutional Avoidance" and held that "[a]llowing a magistrate judge to make the ultimate decision in a matter of such clear constitutional import would raise serious Article III concerns." The same Article III concerns are raised here.

In *Adolph Coors Co. v. Wallace*, 570 F. Supp. 202 (N.D. Cal. 1983), plaintiff company sued a gay activist group that organized a boycott against the company and plaintiff served interrogatories that requested the names of the defendant group's members and financial donors. The Magistrate Judge ordered the group to disclose such information but the District Court Judge reviewed and reversed the order. The Court held that the Constitutional implications of the interrogatories required a determination by an Article III court.

> "A good-faith interjection of First Amendment privilege to a discovery request however, mandates a comprehensive balancing of the plaintiffs' need for the information sought against the defendants' constitutional interests in claiming the privilege. This balancing is of paramount importance, not only in achieving the correct result as between these parties, but also in vindicating the constitutional values which underlie this controversy for all those involved." 570 F.Supp. at 206.

The *Adolph Coors Co.* Court further stated:

> "In cases pitting the government against a private association, the

Supreme Court has required that the government's interest be demonstrated to be 'compelling', and bear a 'substantial relation' to the disclosure sought. Additionally, the government must show that the sought-after disclosure represents the 'least restrictive means' for accomplishing its objectives, and will not unnecessarily sweep constitutional rights aside. Finally, the Court charges us to weigh against the government's interest in disclosure the likelihood of injury to an association, or its members, if the desired information is released.

...

"We are persuaded, by our reading of the Supreme Court's opinion in *NAACP v. Alabama ex rel. Patterson*[19] and the California Supreme Court's pronouncement in *Britt v. Superior Court*,[20] that a private litigant is entitled to as much solicitude to its constitutional guarantees of freedom of associational privacy when challenged by another private party, as when challenged by a government body.

---

[19] 357 U.S. 449, 78 S. Ct. 1163, 2 L. Ed. 2d 1488 (1958).

[20] 20 Cal.3d 844, 574 P.2d 766, 143 Cal. Rptr. 695 (1978).

"This certainly does not mean that a private litigant will not be able to obtain civil discovery from another private litigant over that party's constitutional objections. It does require that any tribunal confronted with facts and arguments similar to those presented here undertake a sensitive evaluation in three steps: (1) ascertain whether the precise material sought by discovery is truly "relevant" to the gravamen of the complaint; (2) if "relevant", the court must balance the rights and interests of each litigant, the particular circumstances of the parties to the

controversy, and the public interest in overriding the private litigants' representations as to resultant injury or to unavoidable need; and, (3) a conclusion that the discovery request, as framed, is the means least inclusive and intrusive for gathering the information to which the party has been deemed entitled."

570 F.Supp. at 208 (most footnotes omitted).

The *Adolph Coors Co.* case dealt with the associational privacy of members of or donors to the gay activist group who might want to remain anonymous. Here, the same right is enjoyed by visitors to Defendants' websites who want to remain anonymous, particularly as to Plaintiffs and the MPAA, and whose rights Defendants are attempting to protect. Accordingly, this Court should carry out the balancing test. As shown below, the Magistrate Judge decided this issue without carrying out a balancing test. The evidence necessary for a balancing test was not introduced. To carry out the balancing test, this Court should receive further evidence pursuant to 28 U.S.C. § 636(b)(1). Defendants are seeking assistance with respect to the presentation of such further evidence from groups that support online Free Speech and privacy rights. Defendants' counsel was unable to discuss the matter fully with responsible individuals in such groups while the Magistrate Judge's Order was sealed.[4]

[4] See footnote 34 at 34:26-28 and 35:23-28 of the Order. The Magistrate Judge stayed enforcement of the Order and unsealed it on June 8, 2007.

2. The Magistrate Judge Failed To Perform an Appropriate Balancing Test Before Overriding the First Right of Visitors to Defendants' Website to Participate in Anonymous Speech.

Anonymous Internet speech is protected by the First Amendment. *Doe v. 2theMart.com*, 140 F. Supp. 2d 1088 (W.D. Wa. 2001); *New.Net, Inc. v. Lavasoft*, 356 F. Supp. 2d 1090, 1107 (C.D. Cal. 2004); and see the Magistrate Judge's Order at 22:16-26.)

As stated in *Adolph Coors Co.*, supra, "[t]he court must balance the rights and interests of each litigant, the particular circumstances of the parties to the controversy, and the public interest in overriding the private litigants' representations as to resultant injury or to unavoidable need."

Here, the Magistrate Judge failed to balance rights and interests. The reasoning of the Magistrate Judge is set forth in the Order at 23:1-7:

> "This court assumes, without decided 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."

The reasoning of the Magistrate Judge is erroneous for several reasons. First, there was no balancing at all. ***Plaintiffs never showed any unavoidable need.*** Rather, the Court apparently determined that a finding of "insubstantial encroachment" sufficed to justify disregarding the First Amendment. Second, encroachment is serious and the palliatives are no more than shreds of protection that do nothing to reduce the chill on free speech. The chill comes from the fact

that, for the first time in the history of the Internet, an independent website is being compelled by a Court to record "Server Log Data" for no reason other than it is an independent torrent site and that Plaintiffs (seen to be equivalent to the MPAA) want that data. The message to Internet users is "we are tracking you" and "we will be tracking you all the time." The message is "stay away from torrent files and peer-to-peer networking or you will get the same treatment."

Taking the second issue first, "masking the IP addresses" does not provide any relief from the chill because the court states at 34:2-3, that "defendants are not, ***at least at this juncture***, ordered to produce such IP addresses in an unmasked/unencrypted form." The clear implication is that unmasked and unencrypted IP addresses may be ordered to be produced later. As discussed below, only unmasked IP addresses have any value. Defendants are ordered to preserve the data for an unmasking order. Few online will expect the last dike to withstand a rising sea. Recording IP addresses, with or without masking, signals the incoming tide that will soon sweep away any "mask" of protection.

The fallacy in the Court's second palliative — "such data does not identify the users of defendants' website" — is more subtle and requires a broader perspective. An IP address is unique to a user's Internet connection. If a user (using the same Internet connection) visits one website twice, the user can be identified as ***the same*** user through the IP address. See the Order at 34:3-7. The same principle applies when a user visits two websites — each website sees the same unique IP address. If data from the two websites is ***aggregated***, the same user is thereby identified as having visited ***both*** websites. This is valuable information, e.g., for advertisers. Aggregation of such information is a major Internet industry. See *In re Doubleclick Inc. Privacy Litigation*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001). Once other Personal Identifying Information, such as name or social security number, is connected with the IP address, all the data is permanently

available to the owner of the database. *Id*.

Defendants are informed and believe that the Motion Picture Association of America ("MPAA"), which Plaintiffs control, has Internet investigative units dedicated to aggregating information about suspected infringers, including their IP addresses. In particular, Defendants are informed and believe that MPAA investigators run "honeypots," which, in this context, are ***torrent sites set up and operated by MPAA agents*** that attract swarms of downloaders, whose IP addresses can be collected and aggregated. Defendants are informed and believe that MPAA investigators participate in swarms of downloaders who have obtained dot-torrent files from torrentspy.com and that MPAA investigators aggregate IP addresses collected from other participants in that swarm. As discussed below in point B.4, Defendants have sought discovery about the honeypots and other Bittorrent resources operated by MPAA investigators, but discovery has been refused.

Using an intentionally-designed institutional architecture, Plaintiffs and the MPAA have constructed a citadel of privilege in which they are concealing evidence of honeypots and IP addresses and databases of personal information on suspected infringers, including history of any use of Torrentspy, plus additional evidence that Defendants need to save their business and protect online Free Speech and privacy and the future of independent Internet development. Defendants are informed and believe that Plaintiffs have all the proof they need as to issues that are defined with respect to the Server Log Data.

In this proceeding, the Magistrate Judge never addressed any ***need*** of the Plaintiffs. Plaintiffs never showed any need. The Magistrate Judge relied on the ***relevance*** of the data.

The Server Log Data is undoubtedly relevant if the IP addresses are included. In such data, IP addresses are connected to torrent files available through Torrentspy that MPAA investigators also download to review for infringement.

Infringers can be identified and connected to other information in the MPAA's database. Identification of infringers who get dot-torrent files from Torrentspy will supposedly support claims that Torrentspy "contributed" to the infringement. Such evidence can be easily accumulated by such means for any general search engine.

If, however, as ordered by the Magistrate Judge "at this juncture," the IP addresses of the visitors are masked or encrypted, the value of the information is hard to discern. It is impossible to ascertain, for example, whether a particular torrent file is being downloaded to a visitor who resides in South America or one who resides in the United States. The latter download is actionable; but the former is not. *Subafilms, Ltd. v. MGM-Pathe Communications Co.*, 24 F.3d 1088 (9th Cir. 1994).

The Court below erred when it failed to perform a true balancing test, when it adopted the approach of Plaintiffs and when it disregarded the Free Speech rights of Torrentspy visitors to participate in anonymous online speech without a true balancing test. "Masking" or "unmasking" simply clouds up the issues; masking is illusory and genuine masking eviscerates the value of the data while hardly lessening the chill on Free Speech and the invasion of the right to surf the web anonymously. This Court should receive further evidence and should review, modify or set aside the Magistrate Judge's Order

3. In Violation of Due Process of Law, and Despite Defendants' Continuing Protests Against the Invasions, the Magistrate Judge Ruled That Defendants and Their Visitors Had "Consented" to Invasions of Privacy, Thus Stripping Away Protections of the Electronic Communications Privacy Act and the Pen Register Act.

In overriding claims of protections under the Electronic Communications Privacy Act and 18 U.S.C. § 2701, the Magistrate Judge relied on an exceptions in

18 U.S.C. § 2702 for ***voluntary*** disclosures,[5] namely consent exceptions in

---

[5] § 2702. Voluntary disclosure of customer communications or records

(a) Prohibitions. Except as provided in subsection (b) or (c)--
(1) a person or entity providing an electronic communication service to the public ***shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service***; and
...
(3) a provider of remote computing service or electronic communication service to the public ***shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.***

(b) Exceptions for disclosure of communications. A provider described in subsection (a) may divulge the contents of a communication--
(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
....
(3) with the ***lawful consent of the originator or an addressee or intended recipient of such communication***, or the subscriber in the case of remote computing service;
....
(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;
(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032);
(7) to ***a law enforcement agency***--
(A) if the contents--
(i) were inadvertently obtained by the service provider; and
(ii) appear to pertain to the commission of a crime; or
(B) [Deleted]
(8) ***to a governmental entity***, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency. (Emphases added.)

§§ 2702(b)(1) and 2702(b)(3). (Magistrate Judge's Order at 23:17.) The Magistrate Judge ruled (Order at 23:18-21):

> "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."

Such a "consent" is in violation of Defendants' rights to due process of law.

There is nothing in § 2702 to support the principle that the Magistrate Judge can require Defendants to consent that information about Defendants' users be turned over to their adversaries. Everything in § 2702 is opposed to such a principle beginning with the title word "voluntary." Nothing could be less "voluntary" than Defendants' production of Server Log Data to Plaintiffs. The invasions are directed at the privacy of website visitors and none has consented to any disclosure. The Magistrate Judge ignores the strict constraints that Congress mandated before disclosures could be made to governmental entities, law enforcement agencies and other organizations that deal with urgent problems, all to protect the truly voluntary nature of any disclosure.

In *FTC v. Netscape Communications Corp.*, 196 F.R.D. 559 (N.D. Cal. 2000), Judge Patel denied the FTC's Motion to Compel seeking production of documents from the service provider that would have revealed the identities of individuals known by screen names and that would have stated the account holders' names, addresses, telephone numbers and billing records, and the length and type of their accounts. The FTC contended that the subpoena was justified by 18 U.S.C. § 2703(c)(1)(C), part of the Stored Communications Act.

> "Section 2703(c)(1)(C) provides in pertinent part that '[a] provider of electronic communication service' shall disclose private customer information to a government entity only in response to 'an administrative

subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena' served by the government entity.'" 196 F.R.D at 560.

The Court rejected the FTC's contention:

"The court cannot believe that Congress intended the phrase 'trial subpoena' to apply to discovery subpoenas in civil cases, thus permitting government entities to make an end-run around the statute's protections through the use of a Rule 45 subpoena. Section 2703(c)(1)(C) is certainly not an exemplar of clear drafting. However, given the weight of the case law and the relevant canons of statutory construction, the court declines the FTC's invitation to interpret the phrase 'trial subpoena' as encompassing a discovery subpoena duces tecum issued under Rule 45." 196 F.R.D. at 561.

In *O'Grady v. Superior Court*, 139 Cal. App. 4th 1423, 1443, 44 Cal. Rptr. 3d 72 (6th Dist. 2006), the Court relied on *FTC v. Netscape*, supra, and held that the Stored Communications Act ("SCA") prohibited plaintiff Apple Computer from serving subpoenas on service providers to discover the identities of persons who had published Apple's "inside information." The Court closely examined the SCA and determined that disclosures of the identities of such persons came within the prohibitions of the SCA and that civil discovery was not authorized by any of the express exceptions.

"Apple would apparently have us declare an implicit exception for civil discovery subpoenas. But by enacting a number of quite particular exceptions to the rule of nondisclosure, Congress demonstrated that it knew quite well how to make exceptions to that rule. The treatment of rapidly developing new technologies profoundly affecting not only commerce but countless other aspects of individual and collective life is

not a matter on which courts should lightly engraft exceptions to plain statutory language without a clear warrant to do so."

There is nothing to distinguish this case from *FTC v. Netscape and O'Grady* and the discovery sought here is subject to the same rule of nondisclosure. See also *Theofel v. Farey-Jones*, 359 F. 3d 1066, 1077 (9th Cir. 2004).

At 24:6-10 of the Order, the Magistrate Judge ruled that a similar "consent" provision authorized violations of The Wiretap Act, 18 U.S.C. §§ 2510-2522. The ruling was erroneous for the same reasons as those applicable to the SCA.

With only a cursory consideration, the Magistrate Judge disregarded the protections of the Pen Register Statute, 18 U.S.C. §§ 3121-27. As the Magistrate Judge correctly noted, this statute prohibits the installation of devices which capture IP addresses. (Order at 25:14-26:2.) "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)." (Magistrate Judge's Order at 26:8-10.)[6]

The Magistrate's Order requires the de facto equivalent of putting a packet

---

[6] § 3121. General prohibition on pen register and trap and trace device use; exception

(a) In general. Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title [18 USCS § 3123] or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(b) Exception. The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service--

(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service...

sniffer or interception device on the front of the Torrentspy.com servers without its consent to intercept user communications. See *Blumofe v. Pharmatrak, Inc. (In re Pharmatrak Privacy Litig.*), 329 F.3d 9, 21 (1st Cir. 2003); *United States v. Councilman*, 418 F.3d 67, 79 (1st Cir. 2005).

The Magistrate Judge's reasoning simply negates the strong protections of the Pen Register Statute and has no support in the text of the exception. There is nothing in the exception that justifies ordering a service provider to install a recording device and such an order is contrary to the clear Congressional intent, namely, to protect users from such devices absent strict judicial oversight. This is shown by comparing the Magistrate Judge's Order with that issued in *In Re Application of the United States of America for an Order Authorizing The Use of a Pen Register And Trap On [xxx] Internet Service Account/User Name [xxxxxxxx@xxx.com]*, 396 F. Supp. 2d 45, 47 (D. Mass. 2005). There, the Court allowed the devices to be installed, but took care to enforce the rule that "the information shall not include the contents of any communication" as required by 18 U.S.C. §§ 3127(3) and 3127(4).

> "An obvious problem occurs when one considers e-mail. That portion of the 'header' which contains the information placed in the header which reveals the e-mail addresses of the persons to whom the e-mail is sent, from whom the e-mail is sent and the e-mail address(es) of any person(s) 'cc'd' on the e-mail would certainly be obtainable using a pen register and/or a trap and trace device. However, the information contained in the 'subject' would reveal the contents of the communication and would not be properly disclosed pursuant to a pen register or trap and trace device. After all, '"contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport or meaning of that communication.' Title 18 U.S.C. §

2510(8)." *Id*., at 48, footnote omitted.

The Court further addressed the issue:

> The use of a pen register to obtain the internet addresses accessed by a person presents additional problems. The four applications presently before me seek the Internet Protocol (IP) addresses which are defined as a "unique numerical address identifying each computer on the internet." The internet service provider would be required to turn over to the government the incoming and outgoing IP addresses "used to determine web-sites visited" using the particular account which is the subject of the pen register.
>
> If, indeed, the government is seeking only IP addresses of the web sites visited and nothing more, there is no problem. However, because there are a number of internet service providers and their receipt of orders authorizing pen registers and trap and trace devices may be somewhat of a new experience, the Court is concerned that the providers may not be as in tune to the distinction between "dialing, routing, addressing, or signaling information" and "content" as to provide to the government only that to which it is entitled and nothing more.
>
> Some examples serve to make the point. As with the "post-cut through dialed digit extraction" discussed, supra, a user could go to an internet site and then type in a bank account number or a credit card number in order to obtain certain information within the site. While this may be said to be "dialing, routing, addressing and signaling information," it also is "contents" of a communication not subject to disclosure to the government under an order authorizing a pen register or a trap and trace

device.

Second, there is the issue of search terms. A user may visit the Google site. Presumably the pen register would capture the IP address for that site. However, if the user then enters a search phrase, that search phrase would appear in the URL after the first forward slash. This would reveal content -- that is, it would reveal, in the words of the statute, ". . . information concerning the substance, purport or meaning of that communication." Title18 U.S.C. § 2510(8). The "substance" and "meaning" of the communication is that the user is conducting a search for information on a particular topic.

396 F.Supp.2d at 48-49.

Accordingly, the Court ordered:

"The disclosure of the 'contents' of communications is prohibited pursuant to this Order even if what is disclosed is also 'dialing, routing, addressing and signaling information.'

"Therefore, the term 'contents' of communications includes subject lines, application commands, ***search queries, requested file names,*** and file paths"

Id. at 50 (emphasis added).

See also *In re United States*, 416 F. Supp. 2d 13 (D.C. Dist. Ct. 2006); *In re United States*, 460 F. Supp. 2d 448 (S.D.N.Y. 2006).

In other words, suppose a criminal investigation were to be directed at an online provider and a government attorney were to request a Court Order for the installation of a "pen register" at the provider's ISP, recording and storing the "server log data" requested here by plaintiffs. Such a Court Order could go so far as to order the recording of IP addresses of those who communicated with the provider but not the contents of the communications. The word "contents" should,

on the foregoing authority, be construed so as to include the name of the .torrent file downloaded or uploaded or search terms related thereto. Hence, the Pen Register Act would prohibit disclosure of both the IP Address of a visitor to a website coupled with identification of any .torrent file uploaded or downloaded (as requested by plaintiffs) or the search terms entered by the visitor.

The Court below violated Defendants' rights to due process under the Fifth Amendment to the United States Constitution when it deprived Defendants of the rights secured to them by Congress in enacting the ECPA and the Pen Register Statute and, especially, when the Magistrate Judge declared that Defendants "consented" to such deprivation of rights. See *Gilmore v. Ashcroft*, 2004 U.S. Dist. LEXIS 4869 (N.D. Cal. 2004) (due process claim for coerced consent of airport travelers to security demands); *Parkes v. County of San Diego*, 345 F. Supp. 2d 1071, 1088 *et. seq.* (S.D. Cal. 2004) (claim for violation of due process rights alleged by mother whose consent to removal of her children from the home was induced by misrepresentations of government officials). The Magistrate Judge's Order should be set aside or modified.

4. In Violation of Due Process of Law, the Magistrate Judge Required Defendants to Prove Matters Where Defendants Have Been Deprived of Discovery.

Throughout the Order, the Magistrate Judge required Defendants to prove matters in order to overcome the apparent presumptions that Plaintiffs were entitled to the Server Log Data they demanded and that Defendants should be compelled to produce that data to Plaintiffs. Some burdens of proof were properly put on Defendants pursuant to authority but others appear to be innovations of the Magistrate Judge.

The manifest due process defect is that Defendants have been required to

prove matters where the evidence needed for such proof has been concealed by Plaintiffs in an institutional "citadel of privilege." Defendants have been defeated in their attempts to obtain such evidence through motions to compel. It is fundamentally unfair to direct a party to prove a matter where that party has been deprived of access to the evidence needed to carry the burden of proof.

In the following matters, Defendants were required to prove facts where they could not obtain the needed evidence:

1. **Disregard of Defendants' loss of good will and business**. The factors included "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 ion 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." (Magistrate Judge's Order at 27:10-28:2, emphasis added.)

2. **Disregard of Dutch Law prohibiting acts ordered by the Court to be performed in the Netherlands.** "The court primarily relies upon the key relevance of the Server Log Data, the specificity of the data sought, ***the lack of alternative means to acquire such information***, and the fact that defendants are United States individuals 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." (Magistrate Judge's Order at 30:7-12, emphasis added.)

3. **Reasons why Defendants are ordered to produce data temporarily stored in RAM**. "The court's decision is 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 burden and cost." (Magistrate Judge's Order at 31:25-28, emphasis added.)

See also *Farber v. Garber*, 234 F.R.D. 186, 190-191 (C.D. Cal. 2006) (party trying to protect his own bank records bore burden of proof to show that information was not available elsewhere, once relevance of the information was demonstrated.)

In the three enumerated matters, the Magistrate Judge's Order implicitly casts the burden of proof onto Defendants as to "the lack of alternative means to acquire such information." This factor parallels factors such as requiring Defendants to dispute "key and potentially dispositive nature of the Server Log Data which would otherwise be unavailable," similar to the burden to prove that information is not available elsewhere in *Farber*.

Defendants have been attempting to obtain the evidence necessary to establish those points, as well as evidence to show that Plaintiffs do not really need the Server Log Data because MPAA investigators, guided by torrent files downloaded from Torrentspy, have participated in swarms of copyright infringers and have acquired IP addresses, which have been aggregated in databases compiled from various sources, including honeypots, and have acquired other evidence of direct infringement by such means. In other words, there are "alternative means to acquire such information" and Plaintiffs and the agents have acquired such information; only such information is being concealed, in part to justify chilling online Free Speech, invading online privacy and deterring independent development of BitTorrent technology.

In particular, Defendants have been attempting to obtain discovery about honeypots and other means through which Plaintiffs have acquired evidence of direct infringement through downloads of dot-torrent files from Torrentspy but Plaintiffs and their agents, the MPAA, have designed their institutional structure and its relationship to litigation so as to enable them to conceal such evidence in a citadel of privilege. The citadel of privilege has multiple means of obstructing and

deflecting any attempt to obtain evidence concealed therein. In fact, Plaintiffs unashamedly make use of the privileges, by directly stating that any evidence provided is given only through "waiver of the privilege" and by making it impossible to investigate the *bona fides* of the privileges or to learn anything about the evidence concealed within the citadel.

Defendants attempted to state their arguments[7] in a motion before the Magistrate Judge to compel the MPAA to produce documents in response to a Rule 45 subpoena:

> "[T]he MPAA has important evidence concerning Internet file-sharing and defendants' alleged involvement therein; but the MPAA has so organized itself that all the evidence is privileged. The MPAA produces evidence only when the MPAA decides to waive its privileges. E.g., "the MPAA made a limited waiver of their work product protections and produced the underlying screenshots and technical data that formed the basis for the specific allegations of the Complaint." (Fallow decl, Ex. at 2:262:5, emphasis added.) Thus, the MPAA belatedly produces two emails from Anderson received after litigation commenced while maintaining the validity of their 'date' objection." [The "date objection" is the refusal of Plaintiffs and the MPAA to produce any documents created after the date the complaint was filed.]

Chief among the methods Plaintiffs and the MPAA use to conceal evidence is

---

[7] Please see Further Memorandum of Points and Authorities in Support of Defendants' Motion to Compel Production of Documents Pursuant to Subpoena to MPAA at 1:8-18 attached as Exhibit W to the accompanying Rothken declaration. The Magistrate Judge refused to allow the document to be filed late.

the "Privilege Log Trap." Plaintiffs and the MPAA produce voluminous Privilege Logs designed to frustrate the purposes of privilege logs. In other words, the Privilege Logs are crafted to avoid rather than to fulfill the obligation to reveal sufficient information as "will enable other parties to assess the applicability of the privilege or protection." Federal Rule of Civil Procedure 26(b)(5)(A).

Thus Defendants have written:

> "The Privilege Logs are designed to frustrate any attempt by defendants to test the validity of the claims of privilege.
>
> "The MPAA produced one Privilege Log on February 22, 2007 (Supp. Smith Decl., Ex. E) and an Amended Privilege Log on April 2, 2007, after defendants served their portion of the Joint Stipulation on the MPAA (Id., Ex. D). As stated in the Supplementary Declaration of Robert Kovsky, 5, in the interim, defendants wrote to plaintiffs' that "The privilege log does not provide substantive information about the subject matter of materials being withheld and there has not been provided any basis for ascertaining the validity of the work product privilege, which is, in many cases, clearly conditional."
>
> Examination of entries in the Privilege Logs shows that there is no information provided that would enable defendants to select which items are pertinent to their inquiries and to evaluate the strength or weakness of the privilege.
>
> Defendants should not be compelled to overcome the institutional structure of privilege that the MPAA has constructed around the evidence and defendants ask the Court to grant the relief requested."[8]

No relief was provided as to the subpoena directed to the MPAA. Thereafter,

---

[8] *Id*., at 4:18-5:5.

the Magistrate Judge, in the Order here in issue, declared that Defendants had failed to prove matters where the evidence concealed by Plaintiffs and the MPAA would possibly have been of importance. Such determinations were violative of Defendants' rights to due process. This Court should review the Order of the Magistrate Judge and modify it or set it aside.

C. The Magistrate's Order Contains Unprecedented Determinations That Are Contrary to Law and That Should Be Reviewed.

1. In an Erroneous Determination, the Magistrate Judge Ruled That "Server Log Data" — Records Defined by Plaintiffs Which Would Come Into Existence Only If Created by Defendants Under Compulsion of the Court's Order — Constitutes "Electronically Stored Information" Under a 2006 Amendment to Fed. Rule of Civil Proc. 34.

From the perspective of electronic jurisprudence, the most serious ruling of the Magistrate Judge was the determination that "The Server Log Data in Issue Is Electronically Stored Information." (Quoting the title of the Point in the Magistrate Judge's Order at 12:1-14:16.) The Magistrate Judge's Order is gravely in error as to the application of law to technology because the Magistrate Judge treats the passage of transient bits of data through a computer's Random Access Memory ("RAM") as equivalent to "electronically stored information" subject to discovery. According to the Magistrate Judge, all the data that passes through a computer's RAM — essentially all the data that the computer handles — becomes a document to be produced in response to a request for documents. The Magistrate Judge's reasoning is even more gravely in error as a matter of jurisprudence. The reasoning is circular, in effect pre-supposing the existence of the Server Log Data and using the presupposition to show the subsequent existence.

The unrecognized but immovable facts are that Defendants will have to collect any such data out of streams of incoming data (not out of bits of historical data in RAM) and create any file, record or document.

Because of confusion in the record and the overriding legal issues, Defendants do not ask for review of the ***facts*** found by the Magistrate Judge as to the "existence" of Server Log Data in RAM in Defendants' computers. However, the facts are false and this Court should be aware of their falsity and of the possible effects of such findings of fact on the future of electronic jurisprudence. Defendant Parker stated the facts about Defendants' system at the hearing, as recorded in the Transcript of Proceedings (Exhibit V to the accompanying Rothken Declaration at 45:8-10, 78:16-24 and 75:21-76:25). To clarify the record, Defendants are submitting the attached Declaration of Wes Parker. Depending on the Court's determinations herein, the Court may decide to receive further evidence pursuant to 28 U.S.C. § 636(b)(1) and the Parker Declaration constitutes an offer of proof as to matters in issue.[9]

[9] In brief, the Declaration shows that what is in RAM is not "Server Log Data" but IP addresses retained from HTTP headers and that any "Server Log Data" is constructed, not out of historical data in RAM, but out of fresh data arriving in streams to the website receives. The Magistrate Judge's Order avoids the technical problems by ordering Defendants to devise the means of compliance using one or more of "multiple methods" that "the record reflects." (Order at 33:18.).

Defendants have done everything they can to keep "Server Log Data" out of their machines, there has never been any "Server Log Data" at Defendants website and there is none now. The "Server Log Data" will come into existence in Defendants' machines only through compliance with a court order to create such data. Actual records require the collection of data from transient RAM, gathering the data together into one file and then storage of the file in a tangible medium. Until then, such data is no better than "virtual data," devoid of actual existence. The fact that Plaintiffs are using a template for their definition based on a "server logging function" does not change the nature of the imposition. Defendants are being "compelled to create, or cause to be created, new documents solely for their production. Federal Rule of Civil Procedure 34 requires only that a party produce documents that are already in existence. *Alexander v. FBI* (D.D.C. 2000) 194 F.R.D. 305, 310." *Paramount Pictures Corp. v. ReplayTV* (C. D. Cal. 2002) CV 01-9358 FMC (Ex) (filed May 30, 2002) 2002 WL 32151632.

As noted by the Magistrate Judge at 16:7 of the Order, Defendants "heavily rely" on the *ReplayTV* case. Defendants submit that there are strong parallels to that case here.

The phrase "Electronically Stored Information" was added to Federal Rule of Civil Procedure 34 in 2006. As noted in the Magistrate Judge's Order at 12:7-14, the Advisory Committee Notes to the 2006 Amendment of Rule 34(a) state that the rule "**applies to information that is fixed in a tangible form**" and that the definition "is expansive and includes any type of information that is stored electronically." The Notes are silent as to any compact unity or functional integrity that the information must have in time or place of fixation. In the light of a generally cautious approach, it would appear that the silence is intentional. ("The wide variety of computer systems in use, and the rapidity of technological change, counsel against a limiting or a precise definition.") Here, the data has no compact

unity or functional integrity in time or place: user requests arrive at random moments and are interwoven with other data transfers.

The Magistrate Judge never grappled with the issue. Instead, jumping to a maximal position, the Magistrate Judge ruled, in effect, that HTTP header data in RAM constitutes "electronically stored information." Under this reasoning, the presumed existence of the historical data in RAM becomes the justification for ordering the creation of the Server Log Data from streams of incoming data. And, so such reasoning continues, because such data can be ordered to be created, it has always, in effect, existed. This is circular reasoning or begging the question. The existence of isolated bits of information in RAM does not suffice to declare the existence of any (or every) file that can be constructed from such bits. Such reasoning would justify every party's attempts to invent "RAM data" that the adversary must collect, record and preserve. There is a way out of the circular reasoning. It is not necessary to try to limit the definition of "electronically stored information" by some verbal formula that will correctly define all present circumstances and anticipate the future. This Court gave a practical rule of determination in ReplayTV, supra:

> "A party cannot be compelled to create, or cause to be created, new documents solely for their production. Federal Rule of Civil Procedure 34 requires only that a party produce documents that are already in existence. *Alexander v. FBI* (D.D.C. 2000) 194 F.R.D. 305, 310."
>
> Further:
>
> "It is evident to the court, based on Pignon's declaration, that the information sought by plaintiffs is not now and never has been in existence. The Order requiring its production is, therefore, contrary to law. See *National Union Elect. Corp. v. Matsushita Elec. Indust. Co.*, 494 F.Supp. 1257, 1261 (E.D. Pa. 1980)." (Footnote omitted.)

The questions in this case should be decided by such a practical rule. The Server Log Data sought by Plaintiffs is not now and never has been in existence. The Magistrate Judge has ordered the creation of documents solely for their production.

The Magistrate Judge's Order's is impractical because, if RAM is considered a document in civil discovery, the foreseeable consequences include escalating preservation letters, expensive and time-consuming discovery wars and risks of sanctions or a spoliation claim against one who refuses to comply with an adversary's demands for "RAM data."

As stated in the Introduction herein, the Magistrate Judge's Order (at 33:15-20) requires Defendants to preserve "Server Log Data", namely:

> "(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." (Magistrate Judge's Order at 3:15-4:1.)

The Server Log Data must be picked out or selected from streams of data that pass through the servers at Defendants' website. Presumptively, such data passes through RAM. As the data is processed, it must be saved in a file or record or it is lost.[10] The undisputed evidence establishes that Defendants have never selected, recorded or preserved log file data in such a form, have never recorded or preserved IP addresses of users in any form, and have always been opposed, on privacy

---

[10] See the Magistrate Judge's Order at 6:1-17, 13:1-8 and 15:21-16:2, e.g., at 6:1-6:6 and 6:13-16: "In general, when a user clicks on a link to a page or a file on a website, the website's server receives from the user a request for the page or the file. The request includes the IP address of the user's computer, and the name of the requested page or file, among other thing." "If the website's logging function is enabled, the web server copies the request into the log file, as well as the fact that the requested file was delivered. If the logging function is not enabled, the request is not retained." (Footnote and citations to Horowitz declaration omitted.)

grounds, to recording IP addresses. (Magistrate Judge's Order at 7:5-8:5.)

To define "electronically stored information," the Magistrate Judge relied on definitions drawn from copyright law in general and *MAI Sys. Corp. v. Peak Computer*, 991 F.2d 511 (9th Cir. 1993), *cert. den.* 510 U.S. 1033. in particular. This case is significant in showing the error in the Magistrate Judge's Order. The existence question here ("Does Server Log Data exist on the Torrentspy system?") was not raised there: the "copyrighted software" was necessarily an existing "work" under the provisions and definitions of the Copyright Act quoted in *MAI* at 991 F.2d 517-18. The question in *MAI* was: if copyrighted software is loaded into RAM, does that transfer constitute a copy? The *MAI* court held that a copy had been made, based on copyright definitions and factual findings (991 F.2d at 518):

> Peak argues that this loading of copyrighted software does not constitute a copyright violation because the "copy" created in RAM is not "fixed." However, by showing that Peak loads the software into the RAM and is then able to view the system error log and diagnose the problem with the computer, MAI has adequately shown that the representation created in the RAM is "sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration."

The reasoning in *MAI* does not apply to this case. In *MAI*, the data in RAM was all in one place in RAM at one time. There was a ***pre-existing work with functional integrity*** in the form of copyrighted software that was being used by the defendant. Here, Defendants are ordered to ***collect bits of RAM data out of data streams*** and to construct a body of data from the bits collected. Defendants are not only ordered to construct the Server Log Data, Defendants are further ordered to create the means to collect, record, store, preserve and process the Server Log Data and to produce the Server Log Data to Plaintiffs. The rule of *ReplayTV* applies

directly. The Magistrate Judge's Order should be set aside pursuant to Rule 72(a).

2. In an Erroneous Determination, The Magistrate Judge Disregarded International Law and Ordered Defendants to Take Steps in The Netherlands That Might Violate the Law of the Netherlands or Other Countries.

The Magistrate Judge disposed of "International Issues" (Magistrate Judge's Order at 28:3). Defendants argued that Plaintiffs were demanding that Defendants collect and preserve Server Log Data of citizens of the Netherlands in violation of the law of the Netherlands, as well as such data of citizens of other nations in violation of the laws of those nations. The law of the Netherlands is of special importance because Defendants' web servers are located in Amsterdam, the Netherlands and because acts to collect Server Log Data must be performed there. The issues are comparable to the choice of law issues in *Wolpin v. Philip Morris, Inc.*, 189 F.R.D. 418 (C.D. Cal. 1999) that the Court ruled were issues subject to review.

The Magistrate Judge ruled: "The court is not persuaded that such concerns should relieve defendants of their obligation to preserve and produce the Server Log Data." (Order at 28:13-15.)

First, the Court found that use could be made of "the entity which has immediate possession of the Server Log Data [and which] has over 25 United States servers." (*Id*., at 29:1-2.) The Magistrate Judge was referring to "Panther" — a third-party provider of file handling services used by Defendants. The Panther issue was discussed at 8:6-10:5 and incorporated into the mandates of the Order pursuant to the terms of footnote 14 on pages 11 and 12.

As noted by the Court in footnote 12 on page 9, Defendants testified that Panther does not and will not carry out the any function with respect to collection or

recording Server Log Data. To comply with the Magistrate Judge's Order, Defendants must discontinue their employment of Panther. Such discontinuance can be accomplished, although Defendants must bear the loss of the competitive advantage gained from employing Panther (50% faster download speed as perceived by the consumer). However, discontinuing Panther means that its facilities are not available to satisfy the Magistrate Judge's Order. There is nothing concrete in the record about any other company that can both produce Server Log Data and also distribute Defendants' files in a fashion similar to that of Panther, while maintaining territorial distinctions sufficient to enable the logging of IP addresses originating only from the United States of America.

The Magistrate Judge also relied on her general finding of "fact that defendants retain the ability to manipulate the routing of the Server Log Data" (Order at 29:4-5) that Defendants challenge in point D, infra.

The Court then listed factors from *Richmark Corp. v. Timber Falling Consultants*, 959 F.2d 1468, 1474-1475 (9th Cir. 1992), where the holder of a default judgment against a Chinese corporation was frustrated in collection efforts by claims by the corporation that disclosure of its financial information was forbidden by Chinese secrecy laws. A chief distinction with the case presented here is that the Magistrate Judge in this case is not violating the privacy or Free Speech rights of Defendants, but of all of Defendants' visitors, who cannot, as a class, be charged with violating Plaintiffs' copyrights or of having done anything to justify such invasions.

The *Richmark* court relied, in part, on *Societe Internationale Pour Participations Industrielles et Commerciales v. Rogers*, 357 U.S. 197 211, 2 L. Ed. 2d 1255, 78 S. Ct. 1087 (1958) (Societe Internationale), where the Court ruled that:

> "petitioner's failure to satisfy fully the requirements of this production order was due to inability fostered neither by its own conduct nor by

circumstances within its control. ***It is hardly debatable that fear of criminal prosecution constitutes a weighty excuse for nonproduction***." (Emphasis added.) 959 F.2d at 1474.

The *Richmark* court adopted the test from a subsequent Supreme Court case, *Societe Nationale Industrielle Aerospatiale v. United States District Court*, 482 U.S. 522, , 107 S. Ct. 2542, 96 L. Ed. 2d 461 (1987):

> "the importance to the investigation or litigation of the documents or other information requested; the degree of specificity of the request; whether the information originated in the United States; the availability of alternative means of securing the information; and the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located."

959 F.2d at 1474. This was the source of some, but not all, of the factors listed by the Magistrate Judge at 29:22-30:1 of the Order.

Although the Magistrate Judge stated that the court had "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," (Order at 30:3-5), no weighing is identifiable in the Magistrate Judge's Order. Defendants contend, as argued above, that no importance to the litigation has been shown, no ***need*** rather than desire or relevance; that the demand for production is totally categorical, covering every visitor to Torrentspy regardless of any connection to the United States, to copyright infringement or to either, and not at all specific; most of the information originates in countries other than the United States; and there are alternative means of securing equivalent information, namely, from MPAA databases acquired from investigations into Torrentspy, honeypots, etc.

There are additional factors identified by the *Richmark* court, including " 'the extent and the nature of the hardship that inconsistent enforcement would impose upon the person," quoting from *United States v. Vetco,* 691 F.2d 1281, 1288.

The Magistrate Judge's Order adds as factors "the degree of hardship on the producing party and whether such hardship is self-imposed." (Order at 30:1-2.)

The factor "whether hardship is self-imposed" apparently refers to *Richmark* at 959 F.2d at 1477, where the court notes: " If [defendant] is likely to face criminal prosecution in the PRC for complying with the United States court order, that fact constitutes a 'weighty excuse' for nonproduction. *Societe Internationale*, 357 U.S. at 211." However, in *Richmark*, defendant's hardship was 'self-imposed" because defendant could have posted a supersedeas bond for the amount due on the judgment pending appeal or could have paid the judgment. *Id*.

Here, it appears that the Magistrate Judge concluded that any hardship imposed on Defendants was self-imposed. This is show by the court's finding of "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." (Magistrate Judge's Order at 30:9-12.)

In other words, if Defendants are ordered to violate the privacy laws of the Netherlands and to commit a crime against privacy in the Netherlands, it is Defendants' own fault because Defendants located their web servers in the Netherlands to benefit from the privacy laws of the Netherlands. This is like saying that a person who relocates to Florida to take advantage of inheritance laws there should *ipso facto* lose the benefit of Florida inheritance laws. An exercise of free, lawful choice is deemed to be grounds for depriving a person of the benefits of that choice. Defendants are not aware on any court of the United States of America that has ever affirmed such a principle. It will have incalculable injurious effects on the

position of the United States vis-à-vis other countries. This Court should review and set aside or modify the Order of the Magistrate Judge.

D. The Magistrate Judge's Order is Clearly Erroneous in Finding, as a Matter of Fact, that "Defendants Have the Ability to Manipulate at Will How the Server Log Data is Routed" and That Finding is the Premise of the Magistrate Judge's Order That Imposes Duties on Defendants Without Regard for the Losses, Costs or Other Burdens That Defendants Must Bear.

The Magistrate Judge's Order is clearly erroneous in finding that "defendants have the ability to manipulate at will how the Server Log Data is routed" (Magistrate Judge's Order at 10:25-26 and 15:9-10; see also 29:4-5.)

The purported evidence in support of this finding is testimony that Defendants are able to, at their will, to include the services of the third-party provider, Panther, in their cache system, or to discontinue the services of that provider. Nothing more. Panther never logged. (See attached Declaration of Wes Parker.)

There is no evidence to sustain the comprehensive, general finding of the Magistrate Judge. The finding is a basis for the imposition of onerous duties on Defendants without regard to the losses, difficulties, costs and burdens of the duties that Defendants must bear. This Court should set it aside.

III.
CONCLUSION

This case and important issues of electronic jurisprudence are being decided in the Discovery Department. A conclusory interpretation that transient RAM is "electronically stored information" threatens to distort developing law. The values on which Defendants stand — online Free Speech and privacy and independent Internet development — have been disposed of without serious consideration.

Previous attempts to obtain discovery have been rebuffed and now the Court imposes burdens of proof that could only be met by obtaining evidence evidently concealed in Plaintiffs' citadel of privilege. Through the Magistrate Judge's Order, Plaintiffs will obtain control of Defendants' website, Plaintiffs will monitor the activity of Defendants' website, Plaintiffs will invade the privacy of Defendants' visitors and Plaintiffs will chill Free Speech on the Internet without any finding that Defendants did anything wrong, or that its DMCA policy was ineffective, or the provision of a bond. No doubt Plaintiffs foresee additional victories in the Final Decree that will multiply their present advantages and complete the subjugation of Defendants' formerly independent website; but everything they really want will already have been obtained.

For the foregoing reasons, this Court should review the Magistrate Judge's Order, should receive new and additional evidence, and set aside, modify or recommit the matter to the Magistrate Judge.

Dated: June 12, 2007

Respectfully submitted,

ROTHKEN LAW FIRM, LLP

By: 

Ira P. Rothken, Esq.

Attorneys for Defendants

PROOF OF SERVICE

I am over the age of 18 years, employed in the county of Marin, and not a party to the within action; my business address is 3 Hamilton Landing, Suite 280, Novato, CA 94949.

On June 12, 2007, I served the within:

MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF DEFENDANTS' OBJECTIONS TO AND MOTION FOR REVIEW OF ORDER RE SERVER LOG DATA

By EMAIL by agreement of the parties, addressed as follows:

Duane Charles Pozza **Katherine A Fallow** **Steven B Fabrizio** Jenner and Block 601 Thirteenth Street NW, Suite 1200 South Washington, DC 20005 202-639-6000 Email: dpozza@jenner.com	**Karen R Thorland** **Walter Allan Edmiston, III** Loeb and Loeb 10100 Santa Monica Blvd, Ste 2200 Los Angeles, CA 90067-4164 310-282-2000 Email: kthorland@loeb.com
Gregory Paul Goeckner **Lauren T Nguyen** Motion Picture Association of America 15503 Ventura Blvd Encino, CA 91436 818-995-6600	

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct. Executed on June 12, 2007.