

1 JENNER & BLOCK LLP
2 STEVEN B. FABRIZIO (*pro hac vice*)
3 sfabrizio@jenner.com
4 KATHERINE A. FALLOW (*pro hac vice*)
5 kfallow@jenner.com
6 DUANE C. POZZA (State Bar No. 225933)
7 dpozza@jenner.com
8 601 Thirteenth Street, N.W.
9 Suite 1200 South
10 Washington, DC 20005
11 Telephone: 202-639-6000
12 Facsimile: 202-639-6066
13 *Attorneys for Plaintiffs*

10 ROTHKEN LAW FIRM LLP
11 IRA P. ROTHKEN (State Bar No. 160029)
12 ira@techfirm.com
13 3 Hamilton Landing, Suite 280
14 Novato, California 94949
15 Telephone: 415-924-4250
16 Facsimile: 415-924-2905
17 *Attorneys for Defendants*

16 UNITED STATES DISTRICT COURT
17 CENTRAL DISTRICT OF CALIFORNIA

17 COLUMBIA PICTURES)	Case No. CV 06-1093 FMC (JCx)
18 INDUSTRIES, INC., DISNEY)	DISCOVERY MATTER
19 ENTERPRISES, INC., PARAMOUNT)	The Honorable Jacqueline Chooljian
20 PICTURES CORPORATION,)	
21 TRISTAR PICTURES, INC.,)	NOTICE OF MOTION AND
22 TWENTIETH CENTURY FOX FILM)	LOCAL RULE 37-1 JOINT
23 CORPORATION, WARNER BROS.)	STIPULATION REGARDING
24 ENTERTAINMENT INC.,)	PLAINTIFFS' MOTION FOR AN
25 UNIVERSAL CITY STUDIOS LLLP,)	ORDER (1) REQUIRING
26 and UNIVERSAL CITY STUDIOS)	DEFENDANTS TO PRESERVE
27 PRODUCTIONS LLLP,)	AND PRODUCE CERTAIN
28 Plaintiffs,)	SERVER LOG DATA, AND (2)
v.)	FOR EVIDENTIARY SANCTIONS
JUSTIN BUNNELL, FORREST)	Date: April 3, 2007
PARKER, WES PARKER, VALENCE)	Time: 9:30 a.m.
MEDIA, LLC, and DOES 1-10,)	Ctrm: 20
Defendants.)	Discovery Cut-off: May 4, 2007
	Pretrial Conf. Date: Oct. 22, 2007
	Trial Date: Dec. 4, 2007

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

TO ALL PARTIES AND THEIR COUNSEL OF RECORD:

PLEASE TAKE NOTICE that on April 3, 2007, Courtroom 20 of the above-entitled Court, located at 312 N. Spring Street, Los Angeles, California 90012, the above-named plaintiffs will and hereby do move the Court for an order requiring defendants to preserve and produce certain server log data, and for evidentiary sanctions.

This Motion is based on the attached Joint Stipulation Regarding Plaintiffs' Motion for an Order Requiring Defendants to Preserve and Produce Certain Server Log Data, and for Evidentiary Sanctions and attached exhibits, all pleadings, papers and proceedings in this action, and such other matters as the Court deems proper. This motion is made following the conference of counsel pursuant to L.R. 37-1 which took place on February 5, 2007 regarding issues relating to the motion, and further communications between counsel.

Dated: March 9, 2007

Respectfully submitted,

JENNER & BLOCK LLP

By: 

KATHERINE A. FALLOW

STEVEN B. FABRIZIO
KATHERINE A. FALLOW
DUANE C. POZZA
JENNER & BLOCK LLP

KAREN R. THORLAND
W. ALLAN EDMISTON
LOEB & LOEB LLP

GREGORY P. GOECKNER
LAUREN T. NGUYEN
15503 Ventura Boulevard
Encino, CA 91436
Attorneys for Plaintiffs

TABLE OF CONTENTS

	<u>Page</u>
1	
2	
3 I. INTRODUCTORY STATEMENTS	1
4 A. Plaintiffs' Introductory Statement.....	1
5 B. Defendants' Introductory Statement.....	4
6	
7 II. ISSUES IN DISPUTE.....	7
8 DOCUMENT REQUESTS AT ISSUE.....	7
9 A. Document Request 10	7
10 B. Document Request 12	8
11	
12 PLAINTIFFS' CONTENTIONS.....	9
13 A. Background	9
14 1. User Request Data and Server Logs.....	9
15 2. Ease and Importance of Preserving Server Log	
16 Data.....	11
17 3. Defendants Have Known From the Outset that the	
18 Server Data is Relevant and Important.....	12
19 B. Argument.....	13
20 1. Defendants' Willful Failure to Preserve the Server	
21 Log Data Constitutes Intentional Spoliation of	
22 Relevant Evidence.	13
23 (a) Once This Suit Was Filed, Defendants Were	
24 Required to Take Affirmative Steps to	
25 Preserve the User Request Data.	14
26 (b) The User Request Data Is Directly Relevant	
27 and Important to Several Issues in This Case.	15
28	

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

2. None of Defendants’ Arguments Justifies Their Failure to Preserve this Important Evidence. 20

(a) Defendants Are Being Asked to Take Minimal Steps to Preserve Existing Data, Not to “Create” New Evidence. 20

(b) Defendants’ “Privacy” Arguments Are Meritless. 22

(c) Defendants’ Claim that They Need Not Preserve Relevant Evidence Because the Information Is Available from Other Sources Is Factually and Legally Wrong 25

3. The Court Should Order Defendants to Preserve and Produce the Server Data Going Forward, and Should Impose Sanctions for Defendants’ Past Spoliation. 26

(a) The Court Should Order Defendants To Preserve Server Log Data Going Forward in the Litigation, and Compel Defendants to Produce that Data. 26

(b) The Court Should Order Evidentiary Sanctions Against Defendants for Their Past Spoliation..... 27

DEFENDANTS’ CONTENTIONS..... 30

A. Plaintiffs are Improperly Trying to Compel Defendants to Create Records. 30

B. The Privacy Concerns and Free Speech Rights of Torrenstspy.com and Its Visitors Are Properly Before the Court..... 37

C. Plaintiffs Should Pursue Their Investigation Through DMCA Subpoenas. 44

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

D. The Court Should Deny Plaintiffs’ Motion for a Preservation Order.46

E. There Was No Spoliation and No Evidentiary Sanctions are Needed.....47

F. The Court Should Award Reasonable Expenses in Favor of Defendants and against Plaintiffs.48

1 infringement alleged by plaintiffs: inducement, contributory infringement, and
2 vicarious infringement.

3 Indeed, defendants themselves have made these issues cornerstones of their
4 defense. Defendants have asserted repeatedly that, as an evidentiary matter,
5 plaintiffs will not be able to prove direct infringement by TorrentSpy users.
6 Defendants also assert that their TorrentSpy website has “commercially significant
7 noninfringing uses” and thus cannot be held liable for contributory copyright
8 infringement under *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S.
9 417, 442, 104 S. Ct. 774, 78 L. Ed. 2d 574 (1984) (“*Sony/Betamax*”).

10 The single best source of evidence on these issues is the website server data
11 that defendants readily could – but are failing to – preserve. Among other things,
12 this server data would show (i) each time any TorrentSpy user downloads a dot-
13 torrent file from the TorrentSpy website, (ii) the dot-torrent file downloaded, (iii) the
14 Internet Protocol (“IP”) address of the user downloading the dot-torrent file, and (iv)
15 the date and time of the download. This information in and of itself would be
16 conclusive evidence of direct copyright infringement. When a user “clicks” a dot-
17 torrent file on defendants’ TorrentSpy website corresponding, for example, to
18 *Pirates of the Caribbean*, the movie *Pirates of the Caribbean* automatically begins
19 to download to that user’s computer – without any further user input or action.
20 Thus, server data evidence revealing that thousands, or perhaps tens of thousands, of
21 TorrentSpy users have downloaded the *Pirates of the Caribbean* dot-torrent file
22 from torrentspsy.com would, without more, prove that defendants’ users have
23 directly infringed the copyrighted motion picture *Pirates of the Caribbean*.

24 The server data, moreover, is the best data with which to conduct statistical
25 analyses that would show the proportion of actual uses of defendants’ website that
26 are infringing. This evidence – expected to show that the overwhelming use of
27 defendants’ site is infringement – would rebut defendants’ argument that TorrentSpy
28 has “commercially significant noninfringing uses,” thereby eliminating defendants’

1 key defense to contributory copyright infringement; it would demonstrate that “the
2 availability of infringing material acts as a draw for customers,” establishing the
3 critical “financial benefit” prong for vicarious liability, *e.g.*, *A&M Records, Inc. v.*
4 *Napster, Inc.*, 239 F.3d 1004, 1023 (9th Cir. 2001) (internal citations and quotation
5 marks omitted); and it would demonstrate that defendants have induced copyright
6 infringement, *i.e.*, that they have acted with an object of fostering infringement.
7 *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 454 F. Supp. 2d 966, 985
8 (C.D. Cal. 2006) (“[T]he staggering scale of infringement makes it more likely that
9 [defendants] condoned illegal use, and provides the backdrop against which all of
10 [defendants’] actions must be assessed.”). This data is unquestionably relevant and
11 very important.

12 Defendants claim that they must protect the “privacy” of their users. But that
13 is a red herring. Even assuming users have some privacy interest in data that they
14 voluntarily send to a third-party website, there is a protective order in place, with an
15 “attorneys’ eyes only” restriction, which should satisfy any privacy concerns.
16 Moreover, with the provisos discussed below, plaintiffs have offered to accept the
17 server data without the IP address information – thus, without any user-identifying
18 information at all. Defendants also claim that, over time, the volume of preserved
19 data would be burdensome to store. That is also a red herring. Plaintiffs have
20 offered to discuss with defendants reasonable sampling protocols to eliminate any
21 “volume” or “burden” concerns, and are willing to provide the storage medium.

22 At bottom, defendants do not want plaintiffs to have this server data evidence
23 because it substantially undermines their defense. But that does not justify
24 intentional spoliation of evidence. Almost any legitimate website would maintain
25 logs of this server data for business reasons. Whatever defendants’ reasons for not
26 preserving this information prior to commencement of this litigation, once the
27 lawsuit was filed, they were obligated to preserve this evidence, even if that meant
28 changing the logging settings on their server software.

1 **B. Defendants' Introductory Statement**

2 Plaintiffs' "Motion for an Order (1) Requiring Defendants to Preserve and
3 Produce Certain Server Log Data, and (2) for Evidentiary Sanctions" (hereinafter
4 "Motion") is false in its factual premise and unprecedented in its reach. There is not
5 now and there has never been the "Server Log Data" that plaintiffs are seeking.
6 There is nothing to "preserve." Plaintiffs are demanding that defendants create new
7 records solely for the purpose of producing those records to plaintiffs.

8 Throughout the Motion, plaintiffs play semantic games to pretend that there is
9 some record of "Server Log Data" that "already exists" and that defendants are
10 "continually erasing important data." (Plaintiffs' Introductory Statement, first
11 paragraph at 1:10 and 1:16.) Plaintiffs' statements are false: No such record of
12 Server Log Data has ever existed. Wes Parker declaration, Exhibit 4 hereto, ¶ 4.

13 Plaintiffs' falsehoods are shown by their distorted language and
14 inconsistencies. As set forth at 3:21 of the Joint Stipulation, plaintiffs "are willing
15 to provide the storage medium" to record the Server Log Data. According to
16 plaintiffs' expert, Ellis Horowitz, "Even if daily server log data required a few
17 gigabytes of storage space, the data could be backed up to a DVD." (Exhibit 2 at
18 5:8-9.) Plaintiffs are willing to provide the storage medium, a series of DVD's, that
19 would hold information about visitors amounting to a "few gigabytes" a day — an
20 enormous amount — because plaintiffs know that the so-called "Server Log Data"
21 has never existed and they know that defendants never used a storage medium for
22 recording it. Plaintiffs further say that "defendants would merely have to 'turn on'
23 the logging function built into their server software." (*Id.*, at 1:13-14.) In their own
24 words, they demand that defendants "turn on" a logging function to create "a few
25 gigabytes" of "daily server log data" that requires a "storage medium" in the form of
26 a DVD. Plaintiffs are pretending that a possibility of creating records equals
27 actually existing records. The fact is that no such records exist. Torrentspy does not
28 record log files. The server's log file recording function is not being used at

1 Torrentspy. (Parker declaration, ¶ 3.)

2 Plaintiffs have invented the falsehoods about “Server Log Data” to evade a
3 key ruling of Judge Cooper in *Paramount Pictures Corp. v. Replay TV*, CV 01-9358
4 FMC (Ex.). In an Order entered on May 31, 2002, Judge Cooper reversed a ruling
5 of the Replay TV Magistrate Judge because that ruling

6 “impermissibly requires defendants to create new data which does not
7 now exist. A party cannot be compelled to create, or cause to be
8 created, new documents solely for their production. Federal Rule of
9 Civil Procedure Rule 34 requires only that a party produce documents
10 that are already in existence. *Alexander v. FBI* (D.D.C. 2000) 194
11 F.R.D. 305, 310.” (Order in *ReplayTV* on Parties’ Motions for Review
12 of Magistrate’s Order at 3:26-4:4, Exhibit A to the Rothken
13 Declaration, Exhibit 3.)

14 Ira P. Rothken, counsel for defendants in this case, appeared in the *ReplayTV*
15 case and brought the *ReplayTV* Order to plaintiffs’ attention. (See Rothken
16 declaration, Exhibit 3 hereto, ¶ 3.)

17 Repeatedly, defendants have advised plaintiffs’ counsel that defendants do
18 not record “Server Log Data” and that defendants have never had records or
19 documents that memorialize “Server Log Data.” Plaintiffs’ counsel know that
20 Torrentspy does not record log files and that the server’s log file recording function
21 is not being used at Torrentspy. (*Id.*, ¶ 4.)

22 As a separate and independent reason to deny plaintiffs’ Motion, there is no
23 justification shown for invading the privacy of defendants’ visitors in the sweeping
24 way plaintiffs are seeking. Both privacy rights and First Amendment rights are at
25 stake. Visitors do not want to be monitored by the MPAA; and *Torrentspy.com* is
26 the Internet equivalent of a public forum. There are no copies of plaintiffs’
27 copyrighted works at *Torrentspy*. To minimize invasions of privacy or chilling free
28 speech, any valid subpoena or other tool of investigation should be narrowly

1 specific as to a particular individual and grounded in concrete, admissible facts, like
2 a subpoena issued pursuant to the Digital Millennium Copyright Act 9 (DMCA), 17
3 U.S.C. § 512(h). The Court should not order sweeping, general intrusions such as
4 plaintiffs are seeking.

5 Plaintiffs want the Court to Order defendants to become involuntary
6 investigators for plaintiffs' "anti-piracy campaign." Information in the "Server Log
7 Data" could conceivably be turned into DMCA search warrants. Potential visitors
8 might learn online in the BitTorrent community of an Order compelling Torrentspy
9 to create records for plaintiff movie studios and shun Torrentspy.com. No
10 protective order would remove the stigma from public consciousness. And the
11 benefits in producing reliable evidence would be slight. Data recorded at
12 Torrentspy.com pursuant to the Order would not have any close relationship to what
13 was going on before the Order. There is no benefit shown to justify the imposition
14 of onerous and damaging burdens on defendants.

15 Plaintiffs' claims about "spoliation of evidence" and their request for
16 evidentiary preclusion sanctions against defendants are based on factually false
17 premises for reasons set forth above. In addition, plaintiffs' arguments should be
18 rejected even if the Court determines that the principal request should be granted,
19 thus ordering recording of "Server Log Data" prospectively. The issue has been ripe
20 for many months and plaintiffs have always known the factual and legal basis for
21 defendants' position: There is no "Server Log Data" and the ReplayTV Order says
22 that defendants do not have to create such "data." Regardless of the Court's ruling
23 now, defendants' position was stated and maintained in good faith. If plaintiffs
24 wanted to contest the issue, they knew it many months ago and they should have
25 pursued it earlier and avoided any "prejudice" arising from website operations that
26 do not record the "Server Log Data" plaintiffs are demanding.

27 Plaintiffs' Motion is factually false and not brought in good faith. Sanctions
28 should be awarded in favor of defendants for having to oppose the Motion.

1 II. ISSUES IN DISPUTE

2 DOCUMENT REQUESTS AT ISSUE

3 A. Document Request 10

4 10. Provide all documents that identify the dot-torrent files that have been
5 made available by, searched for, or downloaded by users of TorrentSpy, including
6 documents that identify the users who have made available, searched for, or
7 downloaded such dot-torrent files.

8 **RESPONSE:**

9 Responding Party objects to this request as calling for the disclosure,
10 implicitly or explicitly, of matters protected from discovery by the attorney-client or
11 attorney-work product privileges. Responding Parties object to this request as
12 calling for the disclosure, implicitly or explicitly, of information protected by
13 defendant's rights of privacy, financial privacy and rights pertaining to proprietary
14 business information, trade secret, confidential business information or
15 competitively-sensitive information. Responding Parties further object to this
16 request based on the right of privacy via statute, constitution, and common law, and
17 as calling for the disclosure of private information, including but not limited to,
18 private financial and other sensitive information, of a consumer.

19 Responding Party objects to this request as unduly burdensome, vague,
20 ambiguous, overbroad, calls for legal conclusion, misleading, calls for improper or
21 premature expert disclosure or opinion testimony, not relevant to any claim or
22 defense in the action, not reasonably calculated to lead to the discovery of
23 admissible evidence and on the ground that information needed to fully respond to
24 this request is in the possession of or equally available to propounding party.

25 Without waiving these objections, Responding Parties respond as follows:

26 After a diligent search and reasonable inquiry, with the exception of a
27 database of torrent files available by a search on TorrentSpy, which will be
28 produced upon entry of an appropriate protective order, Responding Parties are

1 unable to produce documents responsive to this request because such documents, in
2 Responding Parties' possession or control, have never existed.

3 **B. Document Request 12**

4 12. Provide all documents, including server logs, databases of a similar
5 nature, or reports derived from such logs or databases, that you maintain, have ever
6 maintained, or have available that record the activities of TorrentSpy or its users,
7 including documents concerning:

- 8 a. Electronic communications of any type between TorrentSpy and
9 [users];
- 10 b. Logs of user activities; and
- 11 c. Logs or records of dot-torrent files made available, uploaded, searched
12 for, or downloaded on TorrentSpy.

13 **RESPONSE:**

14 Responding Party object[s] to this request as calling for the disclosure,
15 implicitly or explicitly, of matters protected from discovery by the attorney-client or
16 attorney-work product privileges. Responding Parties object to this request as
17 calling for the disclosure, implicitly or explicitly, of information protected by
18 defendant's rights of privacy, financial privacy and rights pertaining to proprietary
19 business information, trade secret, confidential business information or
20 competitively-sensitive information. Responding Parties further object to this
21 request based on the right of privacy via statute, constitution, and common law, and
22 as calling for the disclosure of private information, including but not limited to,
23 private financial and other sensitive information, of a consumer.

24 Responding Party object[s] to this request as unduly burdensome, vague,
25 ambiguous, overbroad, calls for legal conclusion, misleading, calls for improper or
26 premature expert disclosure or opinion testimony, not relevant to any claim or
27 defense in the action, not reasonably calculated to lead to the discovery of
28

1 admissible evidence and on the ground that information needed to fully respond to
2 this request is in the possession of or equally available to propounding party.

3 **PLAINTIFFS' CONTENTIONS**¹

4 **A. Background**

5 **1. User Request Data and Server Logs.**

6 As part of the normal operation of the TorrentSpy website, users send
7 TorrentSpy's web server certain data in order to access pages or files on the website.
8 That data is received and used by the web server to process the users' requests. That
9 data can either be saved in a log file or discarded. Web server programs are
10 generally configured to automatically preserve that data in a log file, but defendants
11 have apparently configured their web server to discard that information instead.

12 Defendants use the web server Microsoft Internet Information Services (IIS)
13 6.0 to run the TorrentSpy website. The IIS web server is a standard web server
14 program used to support a variety of websites, not just torrent sites. Declaration of
15 Ellis Horowitz, dated February 28, 2007("Horowitz Decl."), attached hereto as
16 Exhibit 2, ¶ 9.² The IIS web server program, like virtually all web server programs,

17
18
19 ¹ A copy of the Court's original scheduling order in this case is attached as Exhibit
20 A to the Declaration of Duane C. Pozza, dated March 1, 2007, attached hereto as
21 Exhibit 1 (exhibits to the Pozza Declaration are hereinafter designated "Pozza Ex.
22 ___"); a copy of the Court's January 22, 2007 order modifying the scheduling order
23 is attached as Pozza Exhibit B; a copy of Defendants' Supplemental Objections and
24 Responses to Requests for Production is attached as Pozza Exhibit C; and a copy of
25 defendants' Answer to the Complaint is attached as Pozza Exhibit D.

26 ² Professor Horowitz is currently a full Professor in both the Computer Science and
27 Electrical Engineering Departments at the University of Southern California. He
28 was formerly the Chair of the USC Computer Science Department, and has over 40
years experience as a computer scientist. Professor Horowitz's resume is attached
as Exhibit A to the Horowitz Declaration. Professor Horowitz has testified as an
expert in computer science and software at trial in federal court. Horowitz Decl.,

(continue...)

NOTICE OF MOT. AND L.R. 37-1
J. STIP. RE PLAINTIFFS' MOT. FOR
A PRESERVATION ORDER
AND EVIDENTIARY SANCTIONS

1 contains what is known as “logging functionality.” *Id.* ¶ 10. The logging
2 functionality is built into the IIS web server program; it does not need to be created
3 or modified. That logging functionality works as follows:

4 As a general matter, when a user clicks on a link to a page or a file on a
5 website, the website’s web server program receives from the user a request for the
6 page or the file. This user request contains data that includes the IP address of the
7 user’s computer and the name of the requested page or file. Horowitz Decl. ¶ 11.
8 This information is received by the web server whether or not logging is turned on.

9 In the context of TorrentSpy, a user who wants to download a copy of *Pirates*
10 *of the Caribbean* will first search for that title on the torrentspy.com website. The
11 website will return a number of results. Pozza Ex. E. Once the user clicks on a
12 particular result, torrentspy.com will display certain information about the desired
13 dot-torrent file, and will display a “download torrent” link. Pozza Ex. F. When the
14 user clicks on that “download torrent” link, TorrentSpy’s web server receives the
15 user request – including the data that contains the IP address and name of the
16 requested dot-torrent file – and responds by sending the requested dot-torrent file to
17 the user. As a result of this process, when the BitTorrent system is working as
18 designed, the automatic downloading of the motion picture *Pirates of the Caribbean*
19 begins. Horowitz Decl. ¶ 11. The only way TorrentSpy’s server “knows” where to
20 send the dot-torrent file, and the dot-torrent file to send, is through the information it
21 receives from the user. *Id.* Each time a user clicks on a link to a page or file on the
22 TorrentSpy website, this process occurs. *Id.*

23
24
25 (continued from previous page)

26 Ex. A. Plaintiffs ask that the Court accept him as such an expert for the purposes of
27 this motion.

28

1 Once the web server receives and processes the user request, the normal
2 course is to copy the user request into a log file. However, if the logging
3 functionality is not enabled (as defendants have represented here) then the user
4 request information is lost. *Id.* ¶ 12. Thus, this user request data *already exists* – it
5 is generated by users, received by TorrentSpy’s web server, and utilized by the web
6 server to respond to user requests. The logging functionality allows that information
7 to be preserved by copying it into a log file. *Id.*

8 Website operators, in the usual course of running a website, normally activate
9 the logging functionality and keep server log data or otherwise record detailed data
10 regarding website usage. Horowitz Decl. ¶ 13. In fact, the logging functionality for
11 IIS is usually initially turned on by default when the web server program is installed,
12 and a website operator must take affirmative steps to turn the logging functionality
13 off. *Id.* ¶ 10. It is unusual for a website operator not to keep server log data for at
14 least some period of time, because the server log data is so useful. That data is
15 useful for maintenance and upkeep of the site and to identify and correct any
16 technical problems with the site, and it is also useful to examine website traffic
17 patterns and evaluate the performance of the site. For commercial websites such as
18 TorrentSpy, the server log data is useful to audit and evaluate data relating to
19 advertising on the website. *Id.* ¶ 13.

20 Contrary to standard practices, defendants have apparently *disabled* the
21 logging functionality of their web server program. As a result, the data that would
22 show the downloading activities of TorrentSpy users is being constantly discarded.

23 **2. Ease and Importance of Preserving Server Log Data.**

24 Regardless of their motivation for de-activating the logging function in the
25 past, as a technical matter it would be a trivial task for defendants to activate the
26 logging function now. Defendants’ counsel admitted at the February 13 hearing that
27 it is possible to enable logging that would record such data as the IP addresses and
28 the URL for the requested torrent file. Pozza Ex. G at 27-29. To do this, defendants

1 would need to do little more than change a single setting on the web server program
2 to enable the logging functionality. Horowitz Decl. ¶ 15. They would not need to
3 write a new program or even install new software. *Id.* Activating the logging
4 functionality would impose little to no burden on the defendants and would not
5 impair the normal functioning of the site in any way. *Id.* Nor could the defendants
6 legitimately claim that logging would be somehow burdensome given that most
7 website operators do in fact keep the logging functionality on. *Id.* ¶ 13.

8 Storage of the preserved server log data would not pose an undue burden.
9 Although defendants have suggested that keeping such server log files would be
10 somehow burdensome, website operators commonly back up server log files
11 periodically, such as on a storage device like a CD or DVD. *Id.* ¶ 18. In this case,
12 backing up the server log data to a DVD would involve minimal cost and time.
13 Even if daily server log data required a few gigabytes of storage space, the data
14 could be backed up to a DVD, which can store over four gigabytes of data and can
15 be purchased for under a dollar. The process of backing up this data to a DVD
16 would take around five or ten minutes and would not require any particular technical
17 expertise. *Id.* Plaintiffs readily could supply the storage media and defray the
18 minimal cost of storage. In the parties' discussions on this issue, plaintiffs have
19 further suggested that the parties could agree to the delivery of a representative
20 sample of server data transferred to storage devices for purposes of discovery.
21 Defendants, however, rejected the offer.

22 **3. Defendants Have Known From the Outset that the Server Data is**
23 **Relevant and Important.**

24 Plaintiffs' formal discovery requests were not the first time defendants were
25 put on express notice of the relevance and importance of the server data at issue.
26 Indeed, the filing of the Complaint itself put defendants on notice of their obligation
27 to preserve the server log data. In addition, early in this lawsuit, plaintiffs explicitly
28 advised defendants of the relevance of this data and their obligation to preserve it.

1 Specifically, on May 15, 2006, plaintiffs' counsel wrote to defense counsel "to
2 formally remind [him] of [his] clients' obligation to preserve *all* potentially
3 discoverable evidence related to the litigation" including "[a]ll logs, including
4 without limitation web server access logs" for the TorrentSpy website. Pozza Ex. H.
5 Thus, it is clear that defendants have been continuously discarding the server log
6 data despite having been aware of its relevance and centrality since the inception of
7 this lawsuit nearly a year ago.

8 **B. Argument**

9 Defendants have willfully and in bad faith discarded the user request server
10 log data. They have done so while at the same time making the server data evidence
11 a central part of their defense by arguing that without the very evidence they are
12 erasing, plaintiffs will not be able to meet their burden of proving direct
13 infringement of their copyrighted works; and by further arguing that their
14 TorrentSpy website has sufficient noninfringing uses to invoke the *Sony/Betamax*
15 defense. The importance of this data is thus demonstrated by defendants' own
16 arguments. Plaintiffs therefore ask that the Court order defendants to immediately
17 begin preserving the log data. Further, because this data, once preserved, will
18 constitute key evidence in this case, plaintiffs seek an order compelling defendants
19 to produce the server data after it has been preserved. Finally, because plaintiffs
20 cannot recover the data defendants have already erased, plaintiffs ask the Court to
21 order, as a sanction for the past willful spoliation, that certain facts are conclusively
22 established as to past infringements.

23 **1. Defendants' Willful Failure to Preserve the Server Log Data**
24 **Constitutes Intentional Spoliation of Relevant Evidence.**

25 Defendants' willful failure to preserve server log data – in the face of repeated
26 requests by plaintiffs to do so, and without reasonable basis – constitutes intentional
27 spoliation of evidence. *See Tennison v. City & County of San Francisco*, Nos. 04-
28 0574, 04-1643, 2006 WL 733470, at *38 (N.D. Cal. Mar. 22, 2006) (explaining that

1 spoliation is “the destruction . . . of evidence, or the failure to preserve property for
2 another’s use as evidence in pending or reasonably foreseeable litigation.” (quoting
3 *Byrni v. Town of Cromwell, Bd. of Educ.*, 243 F.3d 93, 107 (2d Cir. 2001))).

4 **(a) Once This Suit Was Filed, Defendants Were Required to**
5 **Take Affirmative Steps to Preserve the User Request Data.**

6 Defendants are and have been obligated to preserve the evidence of specific
7 user requests, and could have easily done so by activating the logging function on
8 their web server. It is well-established that:

9 [a litigant] is under a duty to preserve what it knows, or reasonably
10 should know, is relevant in the action, is reasonably calculated to lead
11 to the discovery of admissible evidence, is reasonably likely to be
12 requested during discovery, and/or is the subject of a pending discovery
13 request.

14 *Wm. T. Thompson Co. v. Gen. Nutrition Corp.*, 593 F. Supp. 1443, 1455 (C.D. Cal.
15 1984); *see also A. Farber & Partners, Inc. v. Garber*, 234 F.R.D. 186 (C.D. Cal.
16 2006) (“[A] litigant has a duty to preserve evidence it knows or should know is
17 relevant to imminent litigation, and a court may sanction a party who destroys or
18 fails to preserve relevant evidence.” (citations omitted)). Accordingly, once
19 defendants were aware of this lawsuit – and certainly no later than when they
20 received plaintiffs’ letter explicitly requesting them to save the data – defendants
21 should have taken affirmative steps to suspend their policy of erasing the log data by
22 re-enabling their server’s log function.

23 Parties are required to alter their document-retention practices and initiate a
24 “litigation hold” – including taking affirmative steps to halt routine destruction of
25 relevant documents – once litigation commences (or sooner, in some cases) in order
26 to preserve relevant evidence. *See Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212,
27 218 (S.D.N.Y. 2003) (“Once a party reasonably anticipates litigation, it must
28 suspend its routine document retention/destruction policy and put in place a

1 'litigation hold' to ensure the preservation of relevant documents."); *see also Hous.*
2 *Rights Ctr. v. Sterling*, No. 03-859, 2005 WL 3320739, at *2 (C.D. Cal. Mar. 2,
3 2005) (same); *In re Napster, Inc. Copyright Litig.*, 462 F. Supp. 2d 1060,
4 1070 (N.D. Cal. 2006) (holding that court could impose sanctions based on party's
5 failure to cease policy of deleting e-mail once duty to preserve attached); *Wm. T.*
6 *Thompson Co.*, 593 F. Supp. at 1447-48 (finding corporate party in violation of its
7 preservation duties when it issued a memo to all personnel stating that they need not
8 alter their standard document retention/destruction policies and relevant documents
9 were destroyed). Defendants' obligation to have ceased erasing the user request
10 data is no different from requiring a party to cease routinely and automatically
11 deleting emails. Indeed, that mandate is even more important here. The server data
12 is not the same as routine business documents that may or may not be a source of
13 relevant evidence. To the contrary, as explained in more detail below, the server
14 data is itself highly probative direct evidence in this case, and likely conclusive of a
15 key issue (direct infringement) that defendants themselves have put into play.

16 **(b) The User Request Data Is Directly Relevant and Important**
17 **to Several Issues in This Case.**

18 There is no question that the server log data of user requests is highly relevant
19 evidence in this case. This data is relevant to numerous claims and defenses in this
20 case, including (1) direct infringement of plaintiffs' copyrighted works by
21 TorrentSpy's users; (2) defendants' secondary liability – under the theories of
22 inducement, contributory and vicarious copyright infringement – for this massive
23 direct infringement; and (3) defendants' (meritless) defenses to plaintiffs' claims for
24 secondary copyright infringement.

25 *First*, the user request data is itself conclusive proof of direct infringement by
26 TorrentSpy users. To prove secondary infringement, plaintiffs must show (1) direct
27 infringement; and (2) a basis on which to hold the defendants liable for that
28 infringement. *See Napster*, 239 F.3d at 1013 n.2. As defendants' counsel readily

1 admitted at the February 13 hearing, “If you turn server logging on, it would log the
2 IP addresses that come to the site and even log each of the URL’s that are clicked
3 on.” Pozza Ex. G at 29. The server log data would show every time a user
4 “clicked” on the button “download torrent” from the TorrentSpy website, thus
5 triggering the *automatic download* of the desired content. Thus, the server data
6 would (without more) enable plaintiffs to identify each of their copyrighted motion
7 pictures and television programs, and how many times they have been infringed.
8 This data is unquestionably key evidence of direct infringement, and plainly relevant
9 to the issue of damages.

10 To be sure, direct infringement should not even be an issue in this case – it is
11 obvious from defendants’ website that the site is used overwhelmingly for the
12 download of infringing content, just as it was obvious as to the sites at issue in the
13 *Grokster* and *Napster* litigations. Invariably, millions of TorrentSpy users a month
14 download, and thereby directly infringe, plaintiffs’ copyrights. The fact of direct
15 infringement is self-evident and beyond reasonable dispute. Defendants however,
16 have repeatedly put the issue of proving direct infringement in dispute – and have
17 done so based on claims that plaintiffs will not be able to marshal the *evidence* of
18 direct infringement. Defendants simply cannot on the one hand argue that evidence
19 of direct infringement is crucial to plaintiffs’ claims and on the other hand
20 continually erase what is far and away the best and most direct source of that
21 evidence. *Cf. Hotaling v. Church of Jesus Christ of Latter-Day Saints*, 118 F.3d
22 199, 204 (4th Cir. 1997) (“[N]o one can expect a copyright holder to prove
23 particular instances of use by the public when the proof is impossible to produce
24 because the infringing [party] has not kept records of public use. To reiterate, a
25 copyright holder should not be prejudiced in this manner, nor should an infringer
26 benefit from its failure to keep records.”); *In re Aimster Copyright Litig.*, 334 F.3d
27 643, 650-51 (7th Cir. 2003) (“[A] service provider that would otherwise be a
28 contributory infringer does not obtain immunity by using encryption to shield itself

1 from actual knowledge of the unlawful purposes for which the service is being
2 used.”).³
3 *Second*, the server log data is relevant to defendants’ secondary liability for
4 their users’ direct infringement. The server log data will show which files
5 TorrentSpy users actually download; in other words, it will show how the site is
6 actually used. Statistical analysis of this data will demonstrate what volume and
7 proportion of the files downloaded from TorrentSpy correspond to infringing copies
8 of copyrighted works. Plaintiffs believe that such analyses will demonstrate that the
9 overwhelming use of defendants’ TorrentSpy site is for copyright infringement.
10 This evidence is directly relevant to each of the theories on which plaintiffs bring
11 their claim for secondary copyright infringement: inducement, contributory
12 liability, and vicarious liability:

13 Inducement. As the Supreme Court has held, “one who distributes a device
14 with the object of promoting its use to infringe copyright, as shown by clear

15 ³ Defendants dispute that plaintiffs can conclusively meet their burden of proof as to
16 direct infringement based solely on the server data. In their view, the server data
17 shows downloads of dot-torrent files, and not completed downloads of plaintiffs’
18 copyrighted motion pictures and television programs. Defendants argue that
19 plaintiffs need conclusive proof of the latter. Plaintiffs disagree. Given that, absent
20 malfunction, when a user clicks on a dot-torrent file, the actual content (the
21 infringing movie) automatically begins to download to the user’s computer,
22 evidence that thousands, and perhaps tens of thousands of users have downloaded a
23 dot-torrent file corresponding to the movie *Pirates of the Caribbean*, would be
24 more than sufficient to prove by a preponderance of the evidence that a TorrentSpy
25 users directly infringed the movie *Pirates of the Caribbean*. Moreover, under
26 defendants’ theory (that plaintiffs’ have to conclusively prove that a user in fact
27 completed the download of the movie *Pirates of the Caribbean*), the server data
28 defendants are erasing would be even more important. From the user IP address
contained in that server data, plaintiffs could identify the real-world name and
address of the infringing TorrentSpy user and conclusively verify that the user in
fact directly infringed the movie *Pirates of the Caribbean*. There simply is no
comparable source for this evidence.

1 expression or other affirmative steps taken to foster infringement, is liable for the
2 resulting acts of infringement by third parties.” *Metro-Goldwyn-Mayer Studios, Inc.*
3 *v. Grokster, Ltd.*, 545 U.S. 913, 919, 125 S. Ct. 2764, 162 L. Ed. 2d 781 (2005). In
4 *Grokster*, the Court discussed several categories of facts that would give rise to an
5 inference that an operator of a peer-to-peer website acted with an intent to induce
6 infringement, including whether the site is used overwhelmingly for copyright
7 infringement, whether the defendants’ business model depends upon this massive
8 copyright infringement, and whether defendants have taken any steps to block or
9 “filter” copyrighted material from their site. 545 U.S. at 939-40. The user request
10 data is directly relevant to each of these categories.

11 The level of infringement on a website in itself provides evidence of an intent
12 to induce infringement, and as Judge Wilson recently held, “provides the backdrop
13 against which all of [the defendants’] actions must be assessed.” *Grokster*, 454 F.
14 Supp. 2d at 985; *see also Grokster*, 545 U.S. at 929. Indeed, the Supreme Court in
15 *Grokster* noted that it is preferable for courts to have evidence of how such sites are
16 *actually* used, instead of just evidence about the *availability* of files for use. *See*
17 *Grokster*, 545 U.S. at 923. The server data that plaintiffs seek would provide
18 precisely that type of important information.

19 Further, evidence that the site is used for massive copyright infringement is
20 also relevant to defendants’ business model, which plaintiffs assert depends on the
21 high volume of users who use TorrentSpy for copyright infringement. The Supreme
22 Court held in *Grokster* that a business model that depended on high-volume use by
23 infringers would provide key evidence supporting an inference of inducement. *See*
24 *id.* at 939-40; *Grokster*, 454 F. Supp. 2d at 989 (“The record shows that [defendants]
25 knew [their] business model depended on massive infringing use, and acted to grow
26 [their] business accordingly.”). And the server data showing overwhelming
27 copyright infringement is relevant to defendants’ incentive *not* to take meaningful
28 steps to filter copyrighted works from their site – because doing so would directly

1 undermine the very purpose of their business. *See Grokster*, 545 U.S. at 939 (noting
2 that failure to filter supports inference of inducement). As Judge Wilson has
3 observed, it is not surprising that secondary copyright infringers like defendants are
4 resistant to copyright filtering, as their “business depend[s] on attracting users by
5 providing them with the ability to pirate copyrighted content.” *Grokster*, 454 F.
6 Supp. 2d at 991.

7 Contributory and vicarious liability. For similar reasons, the user request data
8 is also relevant to the theories of contributory and vicarious liability. In addition to
9 inducement, contributory liability may be established by showing “knowledge” of,
10 and “material contribution” to, copyright infringement. *See Napster*, 239 F.3d at
11 1019-22. As with inducement, evidence that the TorrentSpy site is actually used for
12 massive copyright infringement is directly relevant to the issue of defendants’
13 knowledge for purposes of establishing contributory liability. Likewise, evidence
14 that the site is used overwhelmingly for copyright infringement – and that the large
15 number of pirated works acts as a “draw” to users, who in turn generate defendants’
16 profits through advertising revenues – is highly relevant to vicarious liability, which
17 requires a showing that defendants financially benefit from copyright infringement
18 and have the right and ability to supervise the direct infringement. *Id.* at 1022-23.

19 *Third*, the server data is directly relevant to an affirmative defense raised by
20 defendants. Defendants’ Affirmative Defense No. 29 asserts that “Plaintiffs’ claims
21 are barred under the *Sony* doctrine as the allegedly infringing technology is capable
22 of substantial non-infringing uses.” Pozza Ex. D. The “*Sony* doctrine” refers to
23 *Sony/Betamax* decision, in which the Supreme Court declined to impose secondary
24 copyright liability on the makers of the VCR in light of evidence that the product
25 was capable of “commercially significant noninfringing uses.” 464 U.S. at 442.
26 The “*Sony* doctrine” is a defense only to a claim of contributory copyright
27 infringement, *see Napster*, 239 F.3d at 1022 (*Sony/Betamax* does not apply to
28 vicarious infringement); *Grokster*, 545 U.S. at 936-37 (same as to inducement), and

1 plaintiffs do not believe it applies to contributory infringement in this context as a
2 legal matter. Nevertheless, plaintiffs intend to develop the factual record to show
3 that defendants' TorrentSpy site does not have any "commercially significant
4 noninfringing uses." Analysis of the server data would provide the most accurate
5 evidence of how the site is actually used.

6 **2. None of Defendants' Arguments Justifies Their Failure to Preserve**
7 **this Important Evidence.**

8 **(a) Defendants Are Being Asked to Take Minimal Steps to**
9 **Preserve Existing Data, Not to "Create" New Evidence.**

10 Having discarded critical evidence for nearly a year, defendants attempt to
11 excuse their spoliation by arguing that preservation of the user request data in server
12 logs would be akin to creating "new" evidence. But that argument fundamentally
13 mischaracterizes the nature of the data that plaintiffs are requesting. As explained
14 above, whenever a user clicks on a link for a dot-torrent file on the TorrentSpy
15 website and requests a dot-torrent file for download, the user's web browser sends a
16 request to the TorrentSpy website server – whether logging is turned on or off. The
17 TorrentSpy web server program receives and processes the data contained in the
18 user's request. Indeed, TorrentSpy's web server *must process that data* in order to
19 respond to the user's request and enable downloads of dot-torrent files from the
20 website. Horowitz Decl. ¶¶ 11-12. In other words, this data already exists and
21 defendants affirmatively use it with every user transaction; defendants have simply
22 taken affirmative steps to discard it as soon as it is received.⁴

23

24 ⁴ For these reasons, this case is readily distinguishable from the case cited by
25 defendants, *Alexander v. FBI*, 194 F.R.D. 305, 310 (D.D.C. 2000). In that case, the
26 court held that a party was not required to produce "a list of persons whose FBI
27 reports were requested by the White House" because that specific list never existed
28 in the first place. *Id.*; cf. *Paramount Pictures Corp. v. Replay TV*, No. 01-9358,

28

1 Thus, the data that defendants should be required to preserve is in no sense
2 “newly-created” evidence. And it would be a simple matter for defendants to start
3 preserving that evidence now. The defendants could collect the server log data
4 simply by changing one setting – an existing standard setting – on the web server
5 program to enable the logging functionality. Horowitz Decl. ¶ 15. Further, as
6 explained above, storing the preserved server log data to a DVD or portable hard
7 drive would involve minimal cost and time. *Id.* ¶ 18. In short, requiring defendants
8 to cease erasing this data would impose little, if any, burden on defendants.

9 Because the data already exists, and because switching the logging function
10 back to “on” would impose no undue burden on defendants, defendants’ arguments
11 that they should be permitted to continue to destroy this evidence are particularly
12 unavailing. *See Gonzales v. Google, Inc.*, 234 F.R.D. 674, 683 (N.D. Cal. 2006)
13 (rejecting argument that non-party did not have to “create documents that do not
14 exist” in a case where the non-party had “not represented that it is unable to extract
15 the information requested from its existing systems”); *see also Wm. T. Thompson*
16 *Co.*, 593 F. Supp. at 1446-47 (finding that defendant “could have preserved and
17 retained on computer tape or disk” information that had been destroyed “without
18 undue burden”).

19 _____
20 *(continued from previous page)*

21 2002 WL 32151632, at *2-*3 (C.D. Cal. May 30, 2002) (applying the rule that “[a]
22 party cannot be compelled to create . . . new documents solely for their production”
23 where the party “would be required to undertake a major software development
24 effort, incur substantial expense, and spend approximately four months doing so.”).
25 Here, in contrast, the user requests actually exist and are processed by the web
26 server in order to enable download of the requested dot-torrent files – and could be
27 easily recorded in a log file. Indeed, the logging function is already a part of
28 defendants’ server software and is in fact the *default* setting. Thus, plaintiffs are
requesting that defendants take the necessary steps to preserve certain data, not
create new data.

1 Defendants also argue that the new e-discovery rules support their failure to
2 preserve the server data, but in fact just the opposite is true. While Rule 37(f)
3 provides a safe harbor for a party who “fail[s] to provide electronically stored
4 information lost as a result of the routine, good-faith operation of an electronic
5 information system,” defendants do not qualify for that safe harbor here. Fed. R.
6 Civ. P. 37(f). The advisory committee notes make clear that “good-faith operation”
7 requires “a party’s intervention to modify or suspend certain features of that routine
8 operation to prevent the loss of information, if that information is subject to a
9 preservation obligation.” *Id.* advisory comm. notes (2006). In other words, to
10 qualify for the safe harbor, defendants were required to “suspend” their deactivation
11 of the logging functionality. Indeed, the advisory committee notes explicitly
12 recognize that “[w]hen a party is under a duty to preserve information because of
13 pending or reasonably anticipated litigation, intervention in the routine operation of
14 an information system is one aspect of what it often called a ‘litigation hold.’” *Id.*
15 Additionally, “[t]he good faith requirement of Rule 37(f) means that a party is not
16 permitted to exploit the routine operation of an information system to thwart
17 discovery obligations by allowing that operation to continue in order to destroy
18 specific stored information that it is required to preserve.” *Id.* The new e-discovery
19 rules simply do not allow defendants to continue to destroy relevant evidence that
20 they have an obligation to preserve – especially where, as here, the data is not
21 merely a source of *potentially* relevant evidence, but is itself directly probative of
22 several key issues in this case.

23 **(b) Defendants’ “Privacy” Arguments Are Meritless.**

24 Defendants have also attempted to excuse their failure to preserve relevant
25 evidence by invoking nebulous and poorly-defined user privacy concerns. But their
26 arguments are unavailing. Defendants’ duty to *preserve* relevant server log data is
27 not excused by any privacy concerns, which, in any event, appear to be minimal in
28 this case. And, any potential privacy issues surrounding the production of server log

1 evidence can be resolved by recourse to the protective order or agreements to redact
2 certain information from the production.

3 Because of the nature of website operations generally (and TorrentSpy
4 specifically), the privacy interests of TorrentSpy users in disclosure of their IP
5 addresses is de minimis. Website operators normally keep server log data as part of
6 the routine operation of their websites. Horowitz Decl. ¶ 13. Moreover, every time
7 a user clicks a link on defendants' website, that data, whether preserved or not, is
8 sent to the web server – an external entity – so that the server can operate
9 effectively. *Id.* ¶¶ 11-12. Thus, the data is in existence and voluntarily shared with
10 an outside source. Indeed, by participating in a peer-to-peer network, users are
11 opening their computers and activities up to others. When a TorrentSpy user
12 downloads a file, it automatically also distributes that file to countless other
13 BitTorrent users. The content the TorrentSpy user is downloading, and that user's
14 IP addresses, are exposed to everyone that user downloads from or distributes to. It
15 is well established that no cognizable privacy interests are implicated in these
16 circumstances. *See, e.g., Smith v. Maryland*, 442 U.S. 735, 743-44, 99 S. Ct. 2577,
17 61 L. Ed. 2d 220 (1979) (“[A] person has no legitimate expectation of privacy in
18 information he voluntarily turns over to third parties.”); *Guest v. Leis*, 255 F.3d 325,
19 335-36 (6th Cir. 2001) (“Individuals generally lose a reasonable expectation of
20 privacy in their information once they reveal it to third parties. . . . [C]omputer users
21 do not have a legitimate expectation of privacy in their subscriber information
22 because they have conveyed it to another person – the system operator.”); *In re*
23 *Verizon Internet Servs., Inc.*, 257 F. Supp. 2d 244, 267 (D.D.C. 2003), *rev'd on*
24 *other grounds sub nom. R.I.A.A. v. Verizon Internet Servs., Inc.*, 351 F.3d 1229
25 (D.C. Cir. 2003) (“[I]f an individual subscriber opens his computer to permit others,
26 through peer-to-peer filesharing, to download materials from that computer, it is
27 hard to understand just what privacy expectation he or she has after essentially
28 opening the computer to the world.”); *United States v. Kennedy*, 81 F. Supp. 2d

1 1103, 1110 (D. Kan. 2000) (noting that activation of file sharing mechanism shows
2 no expectation of privacy).

3 Even if there were a greater than de minimis privacy interest at stake, the
4 plaintiffs have offered to put adequate protections in place to alleviate any privacy
5 concerns surrounding the production of server log data. On January 9, the Court
6 entered a protective order stipulated to by the parties. Under that Order, materials
7 may be designated “confidential” or “highly confidential.” Such designations would
8 certainly protect any third-party privacy interests at stake. *See, e.g., Garber*, 234
9 F.R.D at 191 (holding need for discovery outweighed privacy interests where any
10 privacy concerns over the disclosure of financial information could “be protected by
11 a ‘carefully drafted’ protective order”); *ICG Commc’ns, Inc. v. Allegiance Telecom*,
12 211 F.R.D. 610, 614 (N.D. Cal. 2002) (compelling defendants to produce
13 information pertaining to customer files and finding that a protective order would
14 alleviate any privacy concerns).

15 Moreover, revealing the pretextual nature of defendants’ professed privacy
16 concerns, plaintiffs have already offered to accept the server log data initially with
17 IP addresses marked so long as defendants agree to preserve those IP addresses such
18 that plaintiffs could move for their disclosure should the need arise. Even assuming
19 that the disclosure of IP addresses raises any real privacy concerns, masking them,
20 along with the protective order already in place, fully addresses any privacy
21 concern. *See, e.g., Keith H. v. Long Beach Unified Sch. Dist.*, 228 F.R.D. 652, 658
22 (C.D. Cal. 2005) (holding plaintiff’s need for information outweighed privacy
23 interest where there was a protective order entered and personal information could
24 be redacted).

25
26
27
28

1 (c) **Defendants' Claim that They Need Not Preserve Relevant**
2 **Evidence Because the Information Is Available from Other**
3 **Sources Is Factually and Legally Wrong.**

4 Defendants have also suggested that there is an exception to their obligation
5 to preserve and produce evidence where the same information is otherwise available
6 to plaintiffs. That argument is both legally inaccurate and inapplicable to the facts
7 of this case. As a legal matter, the general rule is that party is required to preserve
8 relevant evidence, period. *See Garber*, 234 F.R.D. at 193 (“[A] litigant has a duty to
9 preserve evidence it knows or should know is relevant to imminent litigation[.]”);
10 *Zubulake*, 220 F.R.D. at 218 (“A party or anticipated party must retain all relevant
11 documents . . . in existence at the time the duty to preserve attaches, and any
12 relevant documents created thereafter.”); *see also Abrahamsen v. Trans-State*
13 *Express, Inc.*, 92 F.3d 425, 428 (6th Cir. 1996) (“The rules of discovery . . . do not
14 permit parties to withhold material simply because the opponent could discover it on
15 his or her own.”). In *Zubulake*, the court held that in the narrow circumstances of
16 that case a “litigation hold does not apply to inaccessible backup tapes” except when
17 certain “information contained on those tapes is not otherwise available.” 220
18 F.R.D. at 218. But the server log data here is in no way “inaccessible.” It is readily
19 available and can be preserved by modifying a single setting on the web server.
20 Moreover, as a factual matter, the server log data is not otherwise available to
21 plaintiffs. That data is a record of user interactions with the TorrentSpy server;
22 plaintiffs have no other means of obtaining records of those interactions.

23
24
25
26
27
28

1 **3. The Court Should Order Defendants to Preserve and Produce the**
2 **Server Data Going Forward, and Should Impose Sanctions for**
3 **Defendants' Past Spoliation.**

4 **(a) The Court Should Order Defendants To Preserve Server Log**
5 **Data Going Forward in the Litigation, and Compel**
6 **Defendants to Produce that Data.**

7 The Court plainly has the authority to enter an order requiring defendants to
8 preserve the user request server log data going forward. This authority exists under
9 Federal Rule of Civil Procedure 26, as well as under the Court's inherent power.
10 *See, e.g., Pueblo of Laguna v. United States*, 60 Fed. Cl. 133, 135 (Fed. Cl. 2004)
11 (recognizing "the ability to order evidence preserved" as one of the Court's inherent
12 powers). As one court has explained:

13 This duty of disclosure would be a dead letter if a party could avoid the
14 duty by the simple expedient of failing to preserve documents that it
15 does not wish to produce. Therefore, fundamental to the duty of
16 production of information is the threshold duty to preserve documents
17 and other information that may be relevant in a case.

18 *Danis v. USN Commc'ns, Inc.*, No. 98 C 7482, 2000 WL 1694325, at *1 (N.D. Ill.
19 Oct. 23, 2000).

20 A preservation order is both "necessary and not unduly burdensome" in this
21 case. *Pueblo of Laguna*, 60 Fed. Cl. at 138. First, defendants' past actions – failing
22 to preserve the server log data despite a clear duty to do so – are more than enough
23 to demonstrate the necessity of the entry of an order by the court. *See id.*
24 (explaining that a party can show "that absent a court order, there is significant risk
25 that relevant evidence will be lost or destroyed . . . by demonstrating that the
26 opposing party has lost or destroyed evidence in the past"). Here, defendants have
27 clearly stated that they have not preserved this evidence, and will not absent a Court
28 order. Second, preserving server data is not unduly burdensome. As described

1 above, defendants could collect the server log data simply by modifying one setting
2 on their web server program. Horowitz Decl. ¶ 15.⁵

3 Defendants should be compelled to produce this server data evidence once
4 they have preserved it. Plaintiffs expressly requested this information in their
5 requests for documents. None of the boilerplate objections offered by defendants
6 justifies withholding the data. As explained above, the server data is directly
7 probative of numerous issues in this case, and indeed should be conclusive evidence
8 of direct infringement. For the most part, defendants cite alleged privacy concerns
9 as a basis for withholding this information (to the extent it is preserved), but for the
10 reasons already stated, the alleged privacy concerns – to the extent they have any
11 basis – can be adequately addressed through the protective order and plaintiffs’ offer
12 to receive the data with the IP addresses redacted. Therefore, defendants should be
13 compelled to produce the data to plaintiffs.

14 **(b) The Court Should Order Evidentiary Sanctions Against**
15 **Defendants for Their Past Spoliation.**

16 In addition to requiring defendants to preserve and produce the data going
17 forward, plaintiffs submit that evidentiary sanctions for defendants’ prior willful
18

19 ⁵ The refusal by defendants’ counsel to direct his clients to preserve this evidence is
20 not an isolated incident. To the contrary, it appears to be part of a calculated
21 litigation strategy. Defendants’ counsel is failing to preserve the same information
22 in the case against Gary Fung involving separate BitTorrent sites. *Columbia*
23 *Pictures v. Fung*, United States District Court, Central District of California, Case
24 No. CV-06-5578-SVW (JCx). And defendants’ counsel represented the defendants
25 in another online copyright case, *Arista Records, Inc. v. MP3Board, Inc.*, No. 11
26 CIV 4660, 2002 WL 1997918 (S.D.N.Y. 2002), where (having failed to preserve the
27 server data evidence of direct infringement) defendants successfully opposed
28 summary judgment based in part on an argument that plaintiffs did not present the
evidence that defendants had failed to preserve. *See id.* at *3. Defendants here
should not be permitted to exploit their own spoliation to their advantage in this
manner.

1 spoliation is justified here. Given defendants' duty to preserve the server log data,
2 their willful failure to do so, the relevance of that data, and the prejudice caused to
3 plaintiffs by its loss, sanctions are wholly appropriate.

4 This Court "has the inherent discretionary power to make appropriate
5 evidentiary rulings in response to the destruction or spoliation of relevant evidence."
6 *Glover v. BIC Corp.*, 6 F.3d 1318, 1329 (9th Cir. 1993).⁶ The Court's determination
7 is case-specific and "[t]he sanction should be designed to: (1) deter parties from
8 engaging in spoliation; (2) place the risk of an erroneous judgment on the party who
9 wrongfully created the risk; and (3) restore the prejudiced party to the same position
10 he would have been in absent the wrongful destruction of evidence by the opposing
11 party." *Hous. Rights Ctr.*, 2005 WL 3320739, at *1 (alteration in original) (quoting
12 *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir. 1999) (internal
13 citations and quotation marks omitted)). Other considerations include "(1) the
14 degree of fault of the party who altered or destroyed the evidence; (2) the degree of
15 prejudice suffered by the opposing party; and (3) whether there is a lesser sanction
16 that will avoid substantial unfairness to the opposing party and, where the offending
17 party is seriously at fault, will serve to deter such conduct by others in the future."
18 *Id.* (quoting *Schmid v. Milwaukee Elec. Tool Corp.*, 13 F.3d 76, 79 (3d Cir. 1994)).
19 In general, evidentiary sanctions against defendants are compelled by "the rule that
20 spoliators should not benefit from their wrongdoing." *West*, 167 F.3d at 779.

21 Defendants' failure to preserve the server log data obviously prejudices
22 plaintiffs' case as to past infringement – not least in part *because defendants have*

23 ⁶ Unlike its sanctioning authority under Rule 37(b), the Court may sanction a party
24 under its inherent power absent violation of a court order. *See* Fed. R. Civ. P.
25 37(b)(2) (providing for sanctions when "a party fails to obey an order to provide or
26 permit discovery"); *Unigard Sec. Ins. Co. v. Lakewood Eng'g & Mfg. Corp.*, 982
27 F.2d 363, 367-68 (9th Cir. 1992) (holding inherent-power sanctions proper where
28 the district court was otherwise without power under Rule 37).

1 *made it a central part of their defense.* Notwithstanding that rampant direct
2 infringement is self-evident, defendants have argued that plaintiffs cannot show
3 direct copyright infringement because plaintiffs cannot adduce the necessary
4 evidence. By destroying the best evidence of that infringement, defendants have
5 substantially prejudiced plaintiffs' ability to prove direct infringement for past acts
6 of TorrentSpy user infringement. Such prejudice, caused by defendants' willful
7 spoliation of evidence, necessitates appropriate sanctions. *See Garber*, 234 F.R.D.
8 at 194 (noting that spoliation sanctions are appropriate "if the destruction prejudiced
9 the opposing party").

10 If the Court grants plaintiffs' motion to preserve and to compel, plaintiffs will
11 have the relevant data and should not be prejudiced in this manner as to claims
12 arising after the data is preserved. However, because defendants have continuously
13 destroyed the data since the inception of the lawsuit, plaintiffs have no way of
14 obtaining the historic data. Accordingly, to readdress this prejudice, plaintiffs ask
15 the Court to rule that direct infringement has been established as to all dot-torrent
16 files corresponding to plaintiffs' copyrighted motion picture and television shows
17 that were hosted by defendants' TorrentSpy site from commencement of this action
18 until defendants began logging the user request server data. *See, e.g., Pressey v.*
19 *Patterson*, 898 F.2d 1018, 1024 (5th Cir. 1990) (suggesting that deeming facts
20 admitted may be appropriate sanction on remand after concluding that striking
21 party's answer was too severe); *see also* Fed. R. Civ. P. 37(b)(2)(A) (granting court
22 power to sanction by entering "[a]n order that . . . designated facts shall be taken to
23 be established for the purposes of the action").

24 Indeed, courts have ordered the much harsher sanctions of default or
25 dismissal in equally, if not less, egregious circumstances. *See, e.g., Computer*
26 *Assocs. Int'l, Inc. v. Am. Fundware, Inc.*, 133 F.R.D. 166, 168, 170 (D. Colo. 1990)
27 (awarding default judgment where party "[d]estroy[ed] the best evidence relating to
28 the core issue in the case" – the relevant version of source code necessary to prove

1 opposing party's claim that the spoliating party had copied its product even where
2 the practice of destroying source code was "commonly followed in the industry");
3 *Wm. T. Thompson Co.*, 593 F. Supp. at 1456 (entering default where party's "willful
4 destruction of documents and records . . . deprived [opposing party] of the
5 opportunity to present critical evidence on its key claims to the jury").

6 **DEFENDANTS' CONTENTIONS**

7 **A. Plaintiffs are Improperly Trying to Compel Defendants to Create** 8 **Records.**

9 The single overriding fact is that defendants have never recorded the data that
10 plaintiffs claim must be "preserved." (Wes Parker declaration, Exhibit 4 hereto, ¶
11 3.) Plaintiffs know that the server's log file recording function — what plaintiffs
12 call a "logging function" — is not being used at Torrentspy. (*Id.*; see also Rothken
13 declaration, Exhibit 3 hereto, ¶ 4.)

14 Because Torrentspy does not record the IP addresses of visitors to the
15 website, Torrentspy has never recorded the names of specific dot-torrent files
16 requested by an identified user and Torrentspy has never recorded the date and time
17 a request was received from an identified user. This language is based on plaintiffs'
18 Proposed Order and apparently defines the "Server Log Data" plaintiffs are seeking.
19 (Plaintiffs' Proposed Order; Parker declaration, ¶ 4.)

20 Torrentspy does not record the IP addresses of visitors to the website when
21 they download torrent files or click on a link, what is apparently meant by plaintiffs'
22 phrase, a "user request." Torrentspy has never recorded the IP addresses of visitors
23 to the website during such activity. Torrentspy has never had possession, custody or
24 control of records or documents that show the IP addresses of visitors to the website
25 recorded on account of such activity. (*Id.*)

26 The absence of such "Server Log Data" at defendants' website is the result of
27 policies and customs of defendants not to record such data. Such policies and
28

1 customs have been in force since operations commenced. They have never changed.
2 (*Id.*, at ¶ 5.)
3 Plaintiffs quite clearly understand that no record or document of their desired
4 “Server Log Data” has ever really existed; but plaintiffs are pretending that there is
5 some “virtual” existence that should be treated as if it were real existence. Only
6 through such a subterfuge could they hope to obtain the unprecedented enlargement
7 of discovery rights they are pursuing here. The pretenses reverberate throughout
8 plaintiffs’ portion of the Joint Statement. Plaintiffs declare that: “Technologically,
9 it would be a trivial matter ... to ‘turn on’ the logging function” (Introductory
10 Statement at 1:12-13). Plaintiffs further say that “defendants have apparently
11 *disabled* the logging functionality of their web server program” (Plaintiffs’ sec A.1,
12 just above A.2, emphasis in original.) Plaintiffs declare that “defendants should
13 have taken affirmative steps to suspend their policy of erasing the data log by re-
14 enabling their server’s log function.” (Point B.1.a.) And at all times, “defendants
15 were required to ‘suspend’ their deactivation of the logging functionality.” (*Id.*,
16 quotation marks around “suspend” in the original.) There is nothing *disabled* other
17 than plaintiffs’ powers of reason. Failing to save particular data from a data stream
18 is not the same as “erasing” that data and there is no “policy of erasing.” There
19 never was any enablement of the “logging functionality” plaintiffs say was
20 “disabled.” Plaintiffs are not talking about anything real. The misleading language
21 should not succeed. Plaintiffs are asking the Court to compel defendants to create
22 records that have never been created before and plaintiffs are asking the Court to
23 punish defendants for not having created such records at some prior time.
24 Defendants submit that there is no authority or good reason for imposing such duties
25 or such punishments on defendants.

26 In *Rockwell International Corp. v. H. Wolfe Iron & Metal Co.*, 576 F. Supp.
27 511, 513 (W.D. Pa 1983), the court held:
28

1 “Initially, we find that Randall Wilkoff, a defendant in this civil action,
2 cannot be compelled to create, upon the request of the plaintiff,
3 documentary evidence which is not already in existence in some form.
4 Rule 34(a), Fed.R.Civ.P., the rule under which the request for
5 exemplars was implicitly made, is limited in its scope to documents
6 “which are in the possession, custody or control of the party upon
7 whom the request is served.” “Rule 34 cannot be used to require the
8 adverse party to prepare, or cause to be prepared, a writing to be
9 produced for inspection, but can be used only to require the production
10 of things in existence.” *Soetaert v. Kansas City Coca Cola Bottling*
11 *Co.*, 16 F.R.D. 1, 2 (W.D.Mo. 1954) (citations omitted).”
12 *Rockwell*, supra, was cited in *Alexander v. FBI*, 194 F.R.D. 305, 310
13 (D.C.D.C. 2000), the authority cited in the ReplayTV Order. *Alexander* involved
14 investigations into alleged improprieties occurring in the Clinton White House;
15 however, the principle was the same. Plaintiffs wanted the White House to produce
16 a list of persons whose FBI reports were requested by the White House during Craig
17 Livingstone’s tenure. Plaintiffs here want essentially the same kind of list.

18 “Rule 34 only requires a party to produce documents that are already in
19 existence. See *Rockwell Int’l Corp. v. H. Wolfe Iron and Metal Co.*,
20 576 F. Supp. 511, 511 (W.D.Pa. 1983); see also 8A CHARLES ALAN
21 WRIGHT ET AL., FEDERAL PRACTICE AND PROCEDURE §
22 2210 (2d ed. 1994) (“[A] party can not be required to permit inspection
23 of documents or things that it does not have and does not control.”) A
24 party is not required “to prepare, or cause to be prepared,” new
25 documents solely for their production. See *Rockwell*, 576 F. Supp. at
26 511. Therefore, as there is no evidence that the EOP does in fact
27 possess any list of individuals whose background summaries or FBI
28 reports were requested by the White House from the FBI, the plaintiffs’

1 request to compel such a list is denied.” 190 F.R.D. at 310 (footnotes
2 omitted)

3 As noted above, *Alexander* was cited in the Order in ReplayTV quoted on the
4 second page of defendants’ Introductory Statement. (See Exhibit 3 hereto, Rothken
5 declaration, Exhibit A thereto, at 3:25-4:4.) ReplayTV sold an early version of a
6 personal video recorder market, e.g., like a TIVO. The company provided amenities
7 available at a website through which the developer regularly downloaded software
8 upgrades. Suing for secondary copyright infringement, plaintiffs argued that the
9 website must be used to collect evidence for plaintiffs to use in the litigation. The
10 Court rejected plaintiffs’ attempts and issued the Order referred to above. See also
11 *Khyber Techs. Corp. v. Casio, Inc.*, 2003 U.S. Dist. LEXIS 12450, Civil Action No.
12 99-12468-GAO (D. Mass. 2004), citing *Alexander* on this point.

13 Contrary to these authorities, plaintiffs are asking the Court to order
14 defendants to create records for plaintiffs to use in the litigation. Dissembling,
15 plaintiffs argue that “this data already exists and defendants affirmatively use it with
16 every user transaction; defendants have simply taken affirmative steps to discard it
17 as soon as it is received.” (Text at footnote 4 of Plaintiffs’ Contentions, supposedly
18 distinguishing *Alexander*.) The two uses of “affirmative” do not overlap. The
19 actual “affirmative step” is taken “when the web server program is installed,”
20 according to plaintiffs’ expert witness, Ellis Horowitz (See Exhibit 2, ¶ 10 at 3:10-
21 13.) This shows that there is no “affirmative step” taken with “every user
22 transaction.” Rather, the decision was made once-for-all-time at the beginning. In
23 the case of *Torrentspy.com*, the decision was “No” and has remained “No.” “The
24 policies and customs excluding such recording were in effect when operations first
25 commenced and they have never changed.” Wes Parker declaration, Exhibit 4,
26 hereto, paragraph 5. Defendants oppose being compelled to change that decision to
27 “Yes” for the purpose of providing records to plaintiffs to use in the litigation. (*Id.*,
28 ¶ 7.)

1 Regardless of the technical details set forth in the Horowitz declaration,
2 defendants understand that any website operator can install and use “logging
3 functionality” to produce records that contain data like the “Server Log Data”
4 plaintiffs are demanding in their proposed Order. A website operator who needs to
5 install any such “logging functionality” can find software to meet the need. The
6 facts are that defendants have never installed such “logging functionality” and have
7 no need for it. Defendants do not want it and oppose being ordered to install it and
8 ordered to use it to create records for plaintiffs.

9 There is no authority in support of an Order imposing on defendants a duty to
10 install and maintain a particular “functionality” that has never been installed before
11 for the purpose of creating records to produce to plaintiffs and certainly nothing that
12 overcomes the principles set forth in *Alexander* supra. The possibility that such
13 duties could be imposed on an adversary would lead to a great number of discovery
14 disputes where the demanding party contends that the responding party is bound by
15 a duty to install some computerized “functionality” that produces records for the
16 demanding party. Plaintiffs’ Proposed Order is unprecedented in its reach. It is
17 particularly overreaching in this case where there are important privacy and free
18 speech rights that such an Order would invade.

19 As authority for their proposition, plaintiffs cite *Gonzales v. Google*, 234
20 F.R.D. 674, 683 (N.D. Cal. 2006). That case strongly supports defendants here.
21 The case does not stand for the proposition plaintiffs seem to be asserting, namely,
22 that at some moment and in some way, defendants became obligated to create
23 records for an adversary in litigation. *Gonzales* had unique facts and it involved an
24 unusual use of a subpoena under Rule 45. As background, in *Ashcroft v. ACLU*, 542
25 U.S. 656, 124 S. Ct. 2783 (2004), the Supreme Court affirmed an injunction against
26 enforcement of the Child Online Protection Act (COPA) — which prohibits
27 commercial Internet communications containing material harmful to minors. To
28 overcome the injunction, the government would be required to show that no “less

1 restrictive alternatives” were available to protect children from online indecency,
2 e.g., parent-installed filters. See *Gonzales* at 234 F.R.D. 678-679. Attorney General
3 Gonzales was attempting to use Google as an investigative tool for research
4 pursuant to that mandate and was using a third-party subpoena under Fed.R.Civ.Pro.
5 45. In *Gonzales*, 234 F.R.D. at 683, the Court held “As a general rule, non-parties
6 are not required to create documents that do not exist, simply for the purposes of
7 discovery. *Insituform Tech., Inc. v. Cat Contracting, Inc.*, 168 F.R.D. 630, 633
8 (N.D. Ill. 1996).”

9 As to the privacy issue, at 234 F.R.D. 683, the court noted Google’s concern:
10 “even a perception that Google is acquiescing to the Government’s demands to
11 release its query log would harm Google’s business by deterring some searches by
12 some users. (Opp. at 18.)” At 234 F.R.D. 684, the court concluded that legal
13 safeguards in and of themselves were insufficient to prevent the harm:

14 However, even if an expectation by Google users that Google would
15 prevent disclosure to the Government of its users’ search queries is not
16 entirely reasonable, the statistic cited by Dr. Stark that over a quarter of
17 all Internet searches are for pornography (Supp. Stark Decl. P 4),
18 indicates that at least some of Google’s users expect some sort of
19 privacy in their searches. The expectation of privacy by some Google
20 users may not be reasonable, but may nonetheless have an appreciable
21 impact on the way in which Google is perceived, and consequently the
22 frequency with which users use Google. Such an expectation does not
23 rise to the level of an absolute privilege, but does indicate that there is a
24 potential burden as to Google’s loss of goodwill if Google is forced to
25 disclose search queries to the Government. (footnote omitted).

26 Here, the issue is, paraphrasing *Gonzales*, whether Torrentspy should bear the
27 loss of goodwill if Torrentspy is forced to disclose search queries to the MPAA.”

28 The potential loss in goodwill to Torrentspy is enormous. The loss may depend on

1 the attention given to the Court's Order by online communities interested in these
2 proceedings or in the BitTorrent industry. Some potential website visitors may fear
3 that "Server Log Data" will be released, e.g., in ways that will then result in
4 subpoenas. Indeed, plaintiffs declare in footnote 3 of their Contentions that "From
5 the user IP address contained in that server data, plaintiffs could identify the real-
6 world name and address of the infringing TorrentSpy user and conclusively verify
7 that the user in fact directly infringed the movie." Visitors with no copyright
8 infringement in mind may object to having their activities monitored by the
9 plaintiffs in a copyright infringement suit. Do defendants owe a duty to warn
10 website visitors about the presence of monitoring by plaintiffs; and do defendants
11 owe a duty to warn website visitors about remote dangers?

12 Defendants and Torrentspy.com had their privacy invaded by the MPAA on a
13 prior occasion, as established in the companion case *Bunnell et. al. v. MPAA*, CV-
14 3206 FMC(JCx), and they have no reason to trust the good faith of plaintiffs or the
15 MPAA. Defendants are offended that, after the MPAA paid for documents obtained
16 through violations of their computer security, plaintiffs and the MPAA are trying to
17 use the courts to invade their privacy even more seriously. (Wes Parker declaration,
18 Exhibit 4 hereto, ¶ 7.)

19 At 234 F.R.D. 687-688, the *Gonzales* court wrote, *sua sponte*, of "its concerns
20 about the privacy of Google's users apart from Google's business goodwill
21 argument." Because the Court refused to order production of the "data" sought by
22 the government that implicated privacy, the Court did not feel obliged to resolve that
23 issue or related issues involving of Electronic Communications Privacy Act. The
24 Court ruled that it would not issue "an order compelling Google to disclose search
25 queries of its users." 234 F.R.D. at 688.

26 Plaintiffs were correct to cite *Gonzales v. Google* but the proposition they
27 declare misses the point. The Court's Order in *Gonzales* granted the Attorney
28 General only a tiny portion of what was requested and that was narrowly specific

1 and well defined. The Court carefully protected the privacy rights and perceptions
2 of Google's visitors, even including an "expectation of privacy by some Google
3 users [that] may not be reasonable," as quoted above.

4 **B. The Privacy Concerns and Free Speech Rights of Torrentspy.com and**
5 **Its Visitors Are Properly Before the Court.**

6 Plaintiffs dismiss privacy concerns as "nebulous and poorly-defined" and
7 head their point with the statement that "Defendants' 'Privacy' Arguments Are
8 Meritless." According to plaintiffs, there are "no cognizable privacy interests."

9 Plaintiffs' argument is erroneous, as shown in *Gonzales v. Google*, supra. If
10 Google's visitors are entitled to have their privacy respected, so are Torrentspy's.

11 The Internet provides "the most participatory form of mass speech yet
12 developed," *ACLU v. Reno*, 929 F. Supp. 824 (E.D. Pa. 1996) at 883, upheld in
13 *Reno v. ACLU*, 521 U.S. 844, 870, 138 L. Ed. 2d 874, 117 S. Ct. 2329 (1997). The
14 Courts have consistently affirmed Free Speech rights of Internet users based on the
15 First Amendment to the United States Constitution despite Congressional
16 enactments trying to restrict speech. See, e.g., *Ashcroft v. Free Speech Coalition*,
17 535 U.S. 234, 122 S. Ct. 1389; 152 L. Ed. 2d 403 (2002); *Ashcroft v. ACLU*, 542
18 U.S. 656, 673, 124 S. Ct. 2783, 159 L. Ed. 2d 690 (2004). There is no tendency in
19 the law that favors plaintiffs in their unprecedented attempt to compel defendants to
20 record identifying information about their website visitors and the visitors' activities
21 at the website. See *Quon v. Arch Wireless Operating Company*, 445 F.Supp.2d
22 1116 (C.D. Cal. 2006) (reasonable expectation of privacy held by users of text
23 pagers provided by City employer).

24 Online privacy rights of Torrentspy.com's visitors are further protected by
25 statute. The Electronic Communications Privacy Act, 18 U.S.C.S. §§ 2701 *et. seq.*
26 protects privacy rights such as those being invaded here. See, e.g., *Freedman v.*
27 *America Online, Inc.*, 303 F.Supp.2d 121 (D. Conn. 2004) (civil action based on
28 detectives obtaining AOL's subscriber's identifying information with an invalid

1 search warrant). Courts enforcing subpoenas under the DMCA, such as subpoenas
2 at issue in *Sony Entertainment Group, Inc. v. Does 1-40*, 326 F. Supp. 2d 556, 562,
3 566 (S.D.N.Y. 2004), recognize the right to anonymous speech and respect an
4 “expectation of privacy” even as to specifically identified copyright infringers that
5 have been properly charged with particular infringements. See also *In re Verizon*
6 *Internet Servs., Inc.*, 257 F. Supp. 2d 244 (D. D.C. 2003) at 258-68, rev’d on other
7 grounds, *Recording Indus. Ass’n of America, Inc. v. Verizon Internet Servs., Inc.*,
8 359 U.S. App. D.C. 85, 351 F.3d 1229 (D.C. Cir. 2003).

9 Privacy rights cannot be dismissed in a cavalier fashion such as that proposed
10 by plaintiffs. “Federal Courts ordinarily recognize a constitutionally-based right of
11 privacy that can be raised in response to discovery requests.” *Soto v. City of*
12 *Concord*, 162 F.R.D. 603, 616 (N.D. Cal. 1995).

13 In a multi-factor approach to issues involving an invasion of privacy,
14 “specificity of the discovery request” is an important factor. *Sony Entertainment*
15 *Group*, supra, 326 F.Supp.2d at 565 and 566. Here, plaintiffs’ demands are broad
16 and sweeping rather than specific.

17 To the extent a multi-factor test is used for privacy determinations here, the
18 following facts should be considered: Information in the “Server Log Data” could
19 be turned into DMCA subpoenas directed at visitors to the website. See footnote 3
20 to plaintiffs’ Contentions quoted above and discussion of the DMCA subpoena and
21 17 U.S.C. § 512(h) below. Even the suggestion that such records are being created
22 might unduly burden the site, its visitors, and be antagonistic to its privacy policy ---
23 further, that few people would do searches if they knew their searches (whether it be
24 for sexually related content or other private areas) would be handed over to a third
25 party, thus acting as a de facto mandatory injunction, resulting in reduced searches
26 and reduced traffic to the site. Fearful of plaintiffs and the MPAA, potential visitors
27 might shun Torrentspy.com. No protective order would remove the fear from public
28 consciousness. And the benefits in producing reliable evidence would be slight.

1 Recorded activity at Torrentspy.com pursuant to the Order would not have any close
2 relationship to what was going on before the Order. All kinds of records might be
3 generated as a result of the Order and visitors would likely go to another site where
4 they are not being monitored by the MPAA. There is no benefit shown to justify the
5 imposition of onerous and damaging burdens on defendants.

6 Free speech rights are also of central importance in this case; and free speech
7 rights resonate with privacy rights. Defendants are doing nothing other than
8 speaking on the Internet. Nothing defendants say is copyrighted; there are none of
9 plaintiffs' copyright materials on the Torrentspy website and none of plaintiffs'
10 copyrighted materials pass through the Torrentspy website. Torrentspy provides
11 noncopyrighted URL's and .torrent files to its anonymous visitors. "The anonymity
12 of Internet speech is protected by the First Amendment." *Doe v. 2TheMart.Com,*
13 *Inc.*, 140 F.Supp.2d 1088, 1091 (D. Wash. 2001).

14 Plaintiffs rely heavily on *MGM, Inc. v. Grokster*, 545 U.S. 913, 125 S.Ct.
15 2764 (2005). Defendant in *Grokster* was "the distributor of a product" (125 S.Ct. at
16 2770) and the product was software downloaded to and installed in the user's
17 computer (*Id.*, at 2771). No free speech concerns attended these acts. Here,
18 defendants speak on the Internet and defendants download files that constitute
19 speech⁷. Free speech is at issue here even though free speech was not in issue in
20 *Grokster*.

21
22
23 ⁷ It is well established that information in coded forms like ".torrent files" is
24 entitled to First Amendment protections. *Universal City Studios, Inc. v. Corley*, 273
25 F.3d 429, 445-449 (2nd Cir. 2001). ("Communication does not lose constitutional
26 protection as 'speech' simply because it is expressed in the language of computer
27 code."); see also *Bernstein v. United States Dep't of State*, 922 F. Supp. 1426,
28 1434-36 (N.D. Cal, 1996); *Junger v. Daley*, 209 F.3d 481, 484 (6th Cir. 2000)).
Torrentspy's speech is protected speech.

1 To hide factual embarrassments, plaintiffs invent categories that have a
2 distorted relationship to reality and then plaintiffs try to restrict discourse to those
3 categories. Using a phrase introduced in the Complaint (Exhibit B to the Rothken
4 declaration, Exhibit 3 hereto, at ¶¶ 7-14), plaintiffs' expert Ellis Horowitz identifies
5 the apparent culprit in this infringement action as "the BitTorrent network"
6 (Horowitz declaration, Exhibit 2, at 1:13, 1:24, 2:13, 2:18-19, 2:22-23, 3:1 and 3:2.)
7 At 2:20 of Exhibit 2, Horowitz apparently defines the "BitTorrent Network" as
8 "BitTorrent users who are online at that moment." "[T]he Torrentspy site plays an
9 essential role in the BitTorrent network." (*Id.*, at 3:1-2.) The charge against
10 Torrentspy is as a representative of "the BitTorrent network."

11 Torrentspy provides a means for communication for Internet visitors
12 interested in BitTorrent technology. There are other websites serving the interests
13 of those visitors, some quite like Torrentspy, others quite different. Such websites
14 are visited by "BitTorrent users who are online at that moment," as stated by
15 Horowitz, and who wish to find each other or to find information left by those
16 online earlier. The "BitTorrent Network" is a *community of speakers* and
17 defendants provide the Internet equivalent of a "public forum."

18 "[I]t has been held that a website that is accessible free of charge to any
19 member of the public, which provides a forum where members of the
20 public may read the views and information posted, and also post their
21 opinions on the site is deemed to be a public forum. *Global Telemedia*
22 *Intern., Inc. v. Doe 1*, 132 F. Supp. 2d 1261, 1264 (C.D. Cal. 2001).

23 This is the case because such websites satisfy the requirement that a
24 public forum be a place open to the public where information is freely
25 exchanged." *New.Net, Inc. v. Lavasoft*, 356 F. Supp. 2d 1090, 1107
26 (C.D. Cal. 2004) (inner quotation marks and citation omitted).

27 What plaintiffs want is for defendants to institute rules in the public forum to
28 suit plaintiffs. As their ultimate aim in the litigation, plaintiffs want defendants to

1 censor speech in the public forum, with the duty enforced through penalty of
2 copyright liability. In this Motion, plaintiffs want to impose on defendants the
3 obligation to track the activities of visitors in the public forum and to report the
4 visitors and their activities to plaintiffs for plaintiffs' use. An Order such as
5 plaintiffs seek would have a serious chilling effect on free speech within the
6 BitTorrent community and would invade the rights of Torrentspy and of its visitors
7 to speak freely on the Internet.

8 There remains, of course, the need for the Court to evaluate the kinds of
9 protection to which defendants' speech is entitled. But questions about the kinds of
10 protection cannot be framed by categorical demands for "all IP addresses" of
11 visitors to defendants' website or on the basis of blanket accusations such as
12 "they're all file sharers and copyright infringers and they have no rights," as
13 apparently argued by plaintiffs.

14 Plaintiffs argue that the server log data would be in and of "itself conclusive
15 proof of direct infringement by TorrentSpy users." (Argument B(1)(b).) No one
16 doubts that a copyright infringer could make use of the facilities of the website.
17 Most likely, some do, on a given day. But there are also likely to be as many
18 visitors, or more, who never carry out any infringing act. Should their activities be
19 logged? Nothing but sheer speculation can suggest a percentage of those that visit
20 to infringe plaintiffs' copyrighted works. That percentage will change if plaintiffs
21 obtain the Order they are seeking, but in ways that cannot be measured.

22 Allegations of copyright infringement do not justify broad sweeping
23 intrusions on the privacy of all website visitors. If there is a claim that a particular
24 visitor is contributing to infringement, it is appropriate to seek such information
25 based on the standard governing a DMCA subpoena, which requires a specifically-
26 identified individual and particular facts of copyright infringement. When
27 addressing "direct infringement," as plaintiffs say they must address, Courts enforce
28

1 DMCA subpoenas supported by underlying documents. See, e.g., *Sony*
2 *Entertainment Group, Inc. v. Does 1-40*, 326 F. Supp. 2d 556, 566 (S.D.N.Y. 2004).
3 Other arguments by plaintiffs are obviously devoid of merit. The substantial
4 noninfringing uses of BitTorrent technology will be proved by experts, who will not
5 need to rely on Server Log Data from Torrentspy for their opinions. Plaintiffs
6 refuse to provide evidence about their own use of BitTorrent technology which is
7 *ipso facto* a noninfringing use. (See Order Granting in Part, Denying in Part,
8 Defendants' Motion to Compel Further Responses to Defendants' Request for
9 Production of Document, Set 2 etc." entered on or about February 14, 2007, Exhibit
10 C to the accompanying Rothken declaration, Exhibit 3 hereto as to "C. Request No.
11 26.")

12 Plaintiffs want to use records created and produced pursuant to Court Order to
13 prove "defendants' knowledge for purposes of establishing contributory liability."
14 The means of knowledge, according to plaintiffs, is the equivalent of knowledge and
15 therefore defendants always knew what this compulsory recordkeeping shows.

16 In fact, such "Server Log Data" would prove nothing. The Court Order
17 would have an unforeseeable, possibly drastic effect on traffic at the website that
18 could not be measured. Prospective visitors to Torrentspy.com might be put on
19 notice of the Court's Order and shun the website. Others might visit drawn by
20 notoriety stemming from the Order and click on a few items to see what happens.
21 Defendants may feel obliged to post a notice on the Home Page explaining the
22 intrusions that visitors will suffer; and defendants must expect that many visitors
23 will quickly terminate the contact if so notified. Meanwhile, a curious bystander
24 looking at "the latest thing" would have his or her information recorded. Some
25 visitors, for reasons of rebellion or mischief, might use the site repeatedly for
26 purposes of copyright infringement. Plaintiffs and their trade association, the
27 MPAA, did not scruple from obtaining defendants' personal documents obtained
28 through violations of computer security. (See *Bunnell v. MPAA*, CV 06-3206 FMC

1 (JCx.) Defendants cannot dismiss the possibility that plaintiffs might create a false
2 appearance about the website through programmed visits designed to manipulate the
3 Server Log Data.

4 Plaintiffs ignore the thrust of new e-discovery rules, e.g., discussed in
5 Advisory Committee Notes for 2006 revisions. The new rules call on the courts to
6 adjust to the practical facts of computer systems and to use a common-sense
7 approach. Plaintiffs are living in an imaginary world where failure to install
8 “logging functionality” means “deactivating logging functionality.” Hence,
9 according to plaintiffs, at some point in time, defendants became obligated to install
10 and run “logging functionality” for the benefit of plaintiffs. “[D]efendants were
11 required to ‘suspend’ their deactivation of the logging functionality.” Apparently,
12 “logging functionality” should have been installed when operations started and,
13 therefore, the Court should order it installed now. Defendants demur: the
14 proposition is a non sequitur; the conclusion does not follow from the premise and
15 the premise is false.

16 In opposition to plaintiffs’ argument about new e-discovery rules, defendants
17 assert the common-sense principle that they were never obligated to install or use
18 “logging functionality” and should not be ordered to do so now. There was never
19 anything to preserve; defendants did not violate a preservation duty; and defendants
20 should not be ordered to create records for the sake of delivery to plaintiffs.

21 The issues are larger than plaintiffs’ attempts to oppress the defendants.
22 Plaintiffs are exploiting their position as parties in this suit against a representative
23 of the “BitTorrent Network” to attempt to threaten all persons involved in “the
24 BitTorrent network” and chill all speech on “the BitTorrent network.” All
25 plaintiffs’ embellished prose cannot cover up the simple fact of that attempt. That
26 attempt should not succeed. Plaintiffs’ Motion should be denied.

27
28

1 **C. Plaintiffs Should Pursue Their Investigation Through DMCA Subpoenas.**

2 A recurrent theme in the authorities is that “less damaging alternatives”
3 should be used when privacy and free speech rights are being protected, avoiding
4 the excesses of broad, sweeping demands such as those made by plaintiffs here. For
5 example, the Supreme Court enjoined COPA’s prohibition of Internet
6 communications containing material that was harmful to minors until “less
7 restrictive alternatives” are explored e.g., software and parental filtering. *Ashcroft v.*
8 *ACLU*, 542 U.S. 656, 673 (2004). In *Gonzales v. Google*, supra, the Court denied
9 the order requested by the Attorney General that would have required Google to
10 disclose search queries of its visitors but the Court allowed a smaller study of
11 50,000 URL’s to go forward, because it was possible to institute suitable safeguards
12 for privacy rights in the smaller study. In the ReplayTV Order (Exhibit 3, Rothken
13 declaration, Exhibit A thereto at 5:2-5), the Court held:

14 “The Court does not question the relevance of information concerning
15 how customers of ReplayTV4000 use their units. However, this
16 information can be obtained by plaintiffs by conducting surveys, a
17 traditional method of gleaning customer data in copyright-infringement
18 cases.”

19 The superiority of proceeding pursuant to the DMCA here is shown by a
20 comparison of a subpoena under the DMCA, 17 U.S.C. § 512(h), to a proceeding
21 under Fed.R.Civ.Pro. 27 for a deposition before the action is filed.

22 “Hence, § 512(h), like Rule 27(a), provides a method for preserving,
23 not merely discovering, information essential to a potential lawsuit.

24 Also lacking in merit is Verizon’s argument that Rule 27(a) is
25 distinguished by the possibility of adversarial proceedings contesting
26 the petition. The alleged infringer may receive no notice of a § 512(h)
27 subpoena before his identity is released, but the entity subpoenaed (the
28 service provider) does have the opportunity to contest the subpoena in

1 federal court before it is enforced. See, e.g., *ALS Scan, Inc. v. RemarQ*
2 *Communities, Inc.*, 239 F.3d 619 (4th Cir. 2001) (action addressing
3 service provider's resistance to DMCA subpoena). In other words, §
4 512(h) does not authorize an entirely *ex parte* form of judicial
5 compulsion.”

6 See also *In re Verizon Internet Servs., Inc.*, 257 F. Supp. 2d 244, 254 (D. D.C.
7 2003) at 260-68, rev'd on other grounds, *Recording Indus. Ass'n of America, Inc. v.*
8 *Verizon Internet Servs., Inc.*, 359 U.S. App. D.C. 85, 351 F.3d 1229 (D.C. Cir.
9 2003). See, generally, *Id.*, 260-268.

10 Clearly, defendants want reserve the right “to contest the subpoena in federal
11 court” on particular grounds that may become apparent when the subpoena is
12 served. Without waiving those rights, defendants submit that what plaintiffs
13 legitimately seek here can be obtained through less damaging alternatives.

14 In *Recording Indus. Ass'n of Am. v. Univ. of N.C. at Chapel Hill*, 367 F.
15 Supp. 2d 945 (M.D.N.C. 2005), the Universities asserted the rights of anonymous
16 students whose identities were requested by the RIAA, which claimed them to be
17 copyright infringers. The individuals were known only by screen names but they
18 were traced to the University providers. Under the Digital Millennium Copyright
19 Act, 17 U.S.C. § 512(h), a subpoena can be obtained by filing a copy of a
20 notification given under subsection 512(c)(3)(A) and supporting documents. This
21 “notification” is commonly known as “a DMCA Notice.” At 367 F.Supp.2d 952,
22 the court ruled:

23 “As noted previously, the notification, among other things, requires the
24 copyright holder to identify the alleged works which have been
25 infringed and to identify the material which is claimed to be infringing.
26 Section 512(c)(3)(A)(ii)&(iii). It contains information which allows
27 the service provider to contact the complaining party, verification
28 statements that the allegedly infringing material is not authorized by the

1 copyright owner or the law, and that the complaining party is
2 authorized to act on behalf of the owner or right holder. 17 U.S.C. §
3 512(c)(3)(A)(iv)-(vi). Therefore, there is no doubt that the notification
4 document contains valuable and necessary information in order for a
5 subpoena to be issued. Without the contents of the notification, there
6 would not be a basis for the subpoena, except for a conclusory
7 allegation that the subpoena is sought to obtain the identity of an
8 alleged infringer. 17 U.S.C. § 512(h)(2)(C). Thus, notification
9 information is a crucial part of the subpoena process.”

10 Plaintiffs should be required to propound discovery requests that are specific
11 and particular in ways that are equivalent to DMCA Notices, with the terms set forth
12 above, as a foundational step to obtaining any information resembling that sought
13 here.

14 In responding to any DMCA Notices and discovery requests based thereon,
15 defendants reserve their rights to object on the basis of the DMCA, the ECPA and
16 all other protections recognized for the benefit of those using the Internet, as well as
17 reserving the right to object on grounds particular to the facts of the litigation, e.g.,
18 the lack of timely pursuit of these matters by plaintiffs. Plaintiffs want defendants
19 to produce currently created discovery while refusing to produce discovery
20 supporting their claims that is created after February 23, 2006, the date their
21 Complaint was filed. (See ruling on Request 24, item 2, Order Granting in Part,
22 Denying in Part, Defendants’ Motion to ‘Compel Further Responses to Defendants’
23 Request for Production of Document, Set 2 etc. entered February 14, 2007, Rothken
24 declaration (Exhibit 3 hereto), Exhibit C thereto.)

25 **D. The Court Should Deny Plaintiffs’ Motion for a Preservation Order.**

26 In point B.3, plaintiffs ask the Court “to enter an order requiring defendants to
27 preserve the user request server log data going forward.” The request should be
28 denied because there is nothing to preserve. Presuming the “user request server log

1 data” is the Server Log Data set forth in the Proposed Order, there is no document or
2 record of such data or Data. There are no existing documents or records to preserve
3 that would correspond to plaintiffs’ request. Records of such data or Data would
4 have to be created.

5 Given the factual fallacy in plaintiffs’ Motion, it is difficult to structure the
6 discussion in traditional legal discourse. Cases where there was something to
7 preserve cannot be compared to a case where there is nothing to preserve.

8 In numerous cases, courts deny applications for preservation orders on
9 various grounds. See *Ferrari v. Gisch*, 225 F.R.D. 599, 611 (C.D.Cal. 2004), citing,
10 e.g., *In re Grand Casinos, Inc. Secs. Litig.*, 988 F. Supp. 1270, 1273 (D. Minn.
11 1997) (declining to order the preservation of evidence because “the preservation of
12 evidence in the possession of the parties is statutorily automatic”). Here, plaintiffs
13 are seeking to compel defendants to create records for plaintiffs to use in the
14 litigation. The records will not exist unless defendants are ordered to produce them.
15 Until the Court orders their production, none will be in existence and there will be
16 nothing to preserve.

17 If the Court orders the production of such records, and if records are produced
18 in compliance with the Order, the Court will have no reason to for worry about
19 “preservation.” Plaintiffs’ Motion for a Preservation Order should be denied.

20 **E. There Was No Spoliation and No Evidentiary Sanctions are Needed.**

21 Plaintiffs accuse defendants of “willful spoliation” of evidence Plaintiffs
22 claim that they have suffered prejudice and that “sanctions are wholly appropriate.”

23 Plaintiffs’ pretenses that defendants are engaged in “spoliation” are puerile
24 and transparent. Nothing is “spoliated” other than plaintiffs’ fantasies about Server
25 Log Data that has never existed.

26 Cases cited by plaintiffs all involve a party destroying evidence or allowing
27 evidence to be destroyed. There was no evidence here to be destroyed and none was
28 destroyed. Plaintiffs are talking about “evidence” that never existed.

1 Defendants maintain that there never was a duty to record "Server Log Data"
2 and that no such duty should be imposed prospectively. Defendants also consider
3 the possibility that the Court will order defendants to record the Server Log Data
4 prospectively and that the Court will consider charges of spoliation and the
5 possibility of an evidentiary sanction.

6 With such a possibility in mind, defendants submit that they did not believe
7 they had an obligation to record Server Log Data, based on their custom and
8 practice in not recording such data and in reliance on the rules of law set forth in the
9 ReplayTV Order. The refusal to record Server Log Data was based on defendants'
10 good faith belief that the refusal was justified. Punishment is not merited for such
11 refusal based on apparently valid principles maintained in good faith.

12 Defendants made their position known at the outset of the litigation. There
13 was no reason for the plaintiffs to delay in bringing the matter to a judicial
14 determination. Any "prejudice" suffered by plaintiffs as a result of lost Server Log
15 Data was caused by plaintiffs own tactics.

16 Plaintiffs have a wider audience than defendants in this action. If they obtain
17 the Orders requested here, plaintiffs and the MPAA will be ready to demand that
18 any adversary turn itself into a computerized generator of litigation documents
19 working for the MPAA. One who refuses the demand will be threatened with a
20 penalty for spoliation. The motive is oppressive and the Motion should be denied.

21 **F. The Court Should Award Reasonable Expenses in Favor of Defendants**
22 **and against Plaintiffs.**

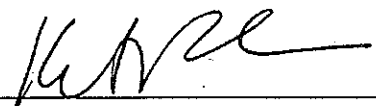
23 Defendants submit that they have been compelled to respond to a voluminous
24 motion that has no merit, that has been filed for purposes of harassment and
25 oppression and that is based on factual falsehoods. An award of reasonable
26 expenses in favor of defendants and against plaintiffs is authorized under
27 Fed.R.Civ.Pro. 37(a)(4)(B). As supported by the Rothken declaration, Exhibit 3
28 hereto, ¶ 7, defendants request an award of \$10,625.00

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Dated: March 9, 2007

Respectfully submitted,

JENNER & BLOCK LLP

By: 

Katherine A. Fallow

STEVEN B. FABRIZIO
KATHERINE A. FALLOW
DUANE C. POZZA
JENNER & BLOCK LLP

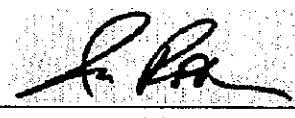
KAREN R. THORLAND
W. ALLAN EDMISTON
LOEB & LOEB LLP

GREGORY P. GOECKNER
LAUREN T. NGUYEN
15503 Ventura Boulevard
Encino, CA 91436

Attorneys for Plaintiffs

Dated: March 12 2007

ROTHKEN LAW FIRM LLP

By: 

Ira P. Rothken

Attorneys for Defendants