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

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

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

COLUMBIA PICTURES INDUSTRIES, INC., DISNEY ENTERPRISES, INC., PARAMOUNT PICTURES CORPORATION, TRISTAR PICTURES, INC., TWENTIETH CENTURY FOX FILM CORPORATION, UNIVERSAL CITY STUDIOS LLLP, UNIVERSAL CITY STUDIOS PRODUCTIONS LLLP, and WARNER BROS. ENTERTAINMENT INC., Delaware corporations, Plaintiffs, vs. JUSTIN BUNNELL, FORREST PARKER, WES PARKER, individuals, VALENCE MEDIA, LLC, a corporation, and DOES 1-10, Defendants.	**Case No. 06-01093 FMC** **DEFENDANTS' FURTHER AND SUPPLEMENTAL MEMORANDUM OF POINTS AND AUTHORITIES IN OPPOSITION TO PLAINTIFFS' MOTION FOR AN ORDER (1) REQUIRING DEFENDANTS TO PRESERVE AND PRODUCE CERTAIN SERVER LOG DATA, AND (2) FOR EVIDENTIARY SANCTIONS AND IN SUPPORT OF DEFENDANTS' REQUEST FOR MONETARY SANCTIONS** Date: April 3, 2007 Time: 9:30 a.m. Ctrm: 20

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

I. Introduction

Pursuant to the Order of the Court dated March 21, 2007, defendants submit this Further and Supplemental Memorandum of Points and Authorities in Opposition to Plaintiffs' Motion re Server Log Data.

Defendants also request that the Court allow defendants to cite Fed.R.Civ.Pro. 37(f), which was overlooked during the preparation of prior Memoranda, and which provides:

> (f) Electronically Stored Information. Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.

II. Response to the Court's Inquiries

The Court has presented five inquiries to defendants which are quoted and answered herein.

> "(i) whether defendants' website receives or possesses (even fleetingly, and even if solely for the purpose of enabling the technical transfer of data) the electronic data in issue (users' IP addresses, identification of torrent file(s) downloaded/ uploaded, date/time of download/upload), and if so, for how long, and if not, how, as a technical matter torrent files are transmitted to/received from website users."

As stated in defendants' Joint Declaration of Justin Bunnell and Wes Parker ("defendants' Joint Declaration), ¶ 5.

> "We currently use Windows IIS software which does indeed have the ability to turn on "logging". We have not turned on such logging to date. If logging was turned on it would capture users' IP address, browser, links tied to the server, date and time of the visit, and click events amongst other things. Without logging turned on the IP addresses

> of users' would likely be fleetingly present in Random Access Memory (RAM) as a method of Internet communication. Regarding the downloading of torrent files no IP address is obtained or was obtained to date through logging or any other means. Since for potential downloads Torrentspy.com provides search results that are hyperlinks to torrent files located on third party servers or caching servers it does not receive or possess even fleetingly users' IP addresses related to such click events. For uploads of torrent files Torrentspy.com obtains via programmatic (non-logging technique) methods the users' IP address without the last octet along with the identification of the torrent file and such files are then, via automated methods, sent to third party caching servers."

"(ii) whether the computer system on which defendants' website currently operates has the capacity, if enabled, to log the electronic data in issue."

As stated in defendants' Joint Declaration, ¶ 6:

> "Yes, logging of electronic data is possible, however, not in any practical way in our current operations. We lease our systems from our Internet Service Provider (ISP) LeaseWeb in Amsterdam, Netherlands, and the equipment is located at the ISP's secure plant. Any hardware changes would need to be approved by LeaseWeb and be in conformity with Netherlands law. (See Choice of Law provision from agreement with LeaseWeb, attached as Exhibit A). The data at issue would accumulate at the rate of about 30-40 gigabytes a day and we currently have no way to store or record such data and we would have to add substantial computing power, bandwidth, and server drive space.
>
> Our servers are currently being driven to near their maximum capacity. Logging would increase the demands put on the computer for each message and the requirements for logging would constitute a

> considerable increase of aggregate demand that would make it impossible for us to sustain our current operations, just because of lack of computational resources. We anticipate that the system will crash several times a day if we are required to log the data in issue, in contrast to the usual rate of about once a week.
>
> Moreover, since defendants' officers are not physically at the server, saving log data would require an FTP download of the files from the server. In our experience, it takes approximately 12 hours to transfer 9 GB of data. At this rate it would be impossible to actually download 30-40GB in a single download day. Assuming an FTP download was accomplished or DVD's were able to be burned at the site of the servers, physical storage, would require approximately ten DVDs to be burned and shipped on a daily basis from servers over seas, requiring an unreasonable amount of processing/burning time and human labor time.
>
> In addition, any such logging would not likely show third party server clickstream."

"(iii) the technical degree of ease or difficulty to enable any such logging function."

As stated in defendants' Joint Declaration, ¶ 7:

> "Please see our response to (ii). Although activation of a logging function would not be difficult, we would have to set up a new system to record and store the data at issue. It is relatively easy to install the software unit called a "logging function" in an operating system and start it running, but this procedure only generates a data stream and says nothing about recording or storing the data in the stream. We would also have to adjust to operating at lower efficiency because of the

> demands placed on the servers and we would have to decide how to deal with the more frequent crashes."

"(iv) the estimated cost (monetary, time, potential loss of business/advertisers, other), and the basis therefor, to (a) enable any such logging function; (b) store/maintain/back-up the data in issue for a one-month period; (c) produce an electronic copy of such data without redaction; and (d) redact users' IP addresses from such data and produce an electronic copy of such redacted data."

> "Requiring defendants to enable a logging function would result in irreparable harm to and loss of business. In particular, recording data from a user's web browser data stream would arguably make defendants' website and servers a "honey pot" or "phishing zone" for companies that have shown a willingness to sue consumers via relationships with the RIAA and MPAA and providing a ready site for locating and obtaining personally identifying information of the users of Torrentspy.com. We also have to comply with applicable law which arguable includes compliance with our privacy policy, Federal law (e.g. ECPA), State law, and the Privacy laws of the Netherlands which require. Amongst other things, robust and specific notice and consent (see e.g. the unofficial translation of the PERSONAL DATA PROTECTION ACT at Article 8 attached as Exhibit B). Moreover, the burden of having to give notice and obtain consent of users to collect such data would be insurmountable. The sheer negative affect of such steps would undoubtedly devastate defendants business, as it would be exposed to significant liability risks, as, for example, AOL has experienced in the recent class action case in which they accidentally disclosed "Member Search Data" (without IP address) and were sued

(see Doe 1 v. AOL, LLC, U.S. District Court, Northern District of California Case No. C 06-5866 SBA, attached as Exhibit C.)

Please see our responses to (ii) and (iii). To record and store the data in issue for any length of time would require us to set up a new server system, possibly in a new location. Even if one could be set up in our present location at our current ISP, re-design of the existing system and installation of new equipment would require a major commitment of money and time. Crudely estimating, two weeks of work and over $10,000 would be required. If we were to terminate our present arrangement with the ISP and set up our own system, the cost would be in excess of $50,000 but the transition might be easier.

An additional installation would be required to produce electronic copies of the data, either with or without redaction of IP addresses. Additional equipment would be required to perform redaction by machine, assuming that software can be written or purchased that scans the data stream and successfully filters IP addresses. The cost for an installation for production of copies would be perhaps 10% to 20% added to the cost for the recording and storing facility, with a higher cost for production with redaction.

Regarding "redaction" the above burdens would still be immense, notice would still likely need to be given since privacy can be impacted via the search query itself, and there would be no practical usefulness of the data in this case. In fact plaintiffs have not established they cannot get data via alternative methods.

As to further issues regarding the potential loss of business/advertisers and other losses, please see the response to inquiry (v), below."

"(v) the degree to which defendants' expressed concerns regarding the privacy of their website users would be impacted if the IP addresses of such users were ordered to be redacted/not produced."

Defendants' state their positions in their Joint Declaration, ¶ 9.

> "If the IP addresses of users were ordered to be redacted or not produced in an order to receive and store server log data, a substantial amount of defendants' privacy concerns would be alleviated. The process would have to be automated in order to be practical, however. The information remaining to defendants would have no relevance in this case, though, as there would be no way to know what the associated torrent files pointed to without IP addresses. Moreover, plaintiffs claim that the alleged infringement of the past is what is at issue, and collecting IP addresses now does not show historical infringement. International privacy laws including US and Netherlands would have to be complied with along with our privacy policy requiring robust notice and consent – this would have a chilling effect on users who would pick another search engine such as Google who did not have such burdens.
>
> Even with the redaction of IP addresses, we are nonetheless opposed to being compelled to serve as investigators for plaintiffs and the MPAA in any capacity whatsoever or as to any information whatsoever unless the MPAA complies with the current DMCA policy. Our opposition does not depend on what information is recorded and produced to plaintiffs. Obviously, reports that include the IP addresses of visitors are more offensive than reports that do not include such IP addresses. Overriding that distinction, being required to record, store and produce any reports whatsoever of any activities of website visitors whatsoever, including the server log data at issue, with or without IP addresses, would violate the privacy of our website visitors and would violate our privacy

policy as well.

We understand that we are being sued as a representative of the BitTorrent community that plaintiffs call “the BitTorrent network” and we understand that “the BitTorrent network,” as defined by plaintiffs, includes (1) individual persons using BitTorrent technology to exchange files, the “users;” (2) operators of .torrent search engines like ours; and (3) operators of BitTorrent tracker sites. Speaking as representatives of the BitTorrent community, with the expert practical knowledge of and experience in Internet development and BitTorrent technology that is needed to and that does make Torrentspy a top website, and based just on what we read online, members of the BitTorrent community are collectively opposed to investigations, legal threats and legal actions instigated by plaintiffs and the MPAA. Based just on what we read online, members of the BitTorrent network are collectively opposed to being tracked online or to having any of their activity recorded and/or to having information about them gathered and/or aggregated by large, rich and/or powerful interests, like the plaintiffs. Nothing in our personal contacts with other members of the BitTorrent community or drawn from our other sources of knowledge creates any doubt about these facts.

Our expectation is that the typical visitor to the Torrentspy website would be opposed to having any record whatsoever of his or her visit, and especially so if any part of that record were to be disclosed to plaintiffs and/or the MPAA. Our expectation is that we would suffer a substantial loss of traffic and a correspondingly loss of income (that is based on traffic) just by reason of being compelled to record visits of users, assuming one operated with integrity and thus that visitors know that their activities are being recorded and that records of their visit will be produced to

> plaintiffs during copyright litigation. Our expectation is that an Order compelling us to record information about visits to our website and to deliver the records to plaintiffs during copyright litigation would be seen by many as a stigma and that many would be disaffected by it. We would be placed at a competitive disadvantage with respect to our competitors in a business where such a competitive disadvantage can quickly become fatal. Indeed those with knowledge can perform searches to try to demonstrate "infringement." We cannot foresee the degree of disaffection, e.g., by advertisers who might no longer want to deal with us, or the degree of loss, given the uniqueness of the situation, but an economic catastrophe cannot be excluded."

In addition to the foregoing, defendants rely on the following point and the additional authorities cited in support thereof.

A. Federal Statutes Protect the Privacy of the Information at Issue and Strengthen Defendants' Position as Guardians of that Information.

The Electronic Communications Privacy Act ("ECPA") is divided into Title I, commonly known as the Wiretap Act, 18 U.S.C. §§ 2510-2522, and Title II, commonly known as the Stored Communications Act, 18 U.S.C. §§ 2701-2711. *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002) *cert. den.* 537 U.S. 1193 (2003). Defendants also rely on the Pen Register Statute, 18 U.S.C. §§ 3121-3127.

Defendants submit that the Wiretap Act prohibits the disclosure of the contents of communications in transit, as here, (18 U.S.C. § 2511(1)(a), (c) and (d)), that the Stored Communications prohibits the disclosure of contents of communications "or other information pertaining to a ... customer" (18 U.S.C. §

2702(a)), and that the Pen Register Statute prohibits the disclosure of identities of persons communicating with a targeted person except to a government attorney acting under stringent judicial oversight (18 U.S.C. § 18219(a)). There is no exception from these prohibitions for civil discovery, although an online service provider might be expected to act in compliance with a directive from a governmental officer or in response to a court order, e.g., obtaining immunity from a civil lawsuit. See 18 U.S.C. §§ 2511(a)(2), 2703(c), 2707(e) and 18 U.S.C. § 3124(e).

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

> "Section 2703(c)(1)(C) provides in pertinent part that '[a] provider of electronic communication service' shall disclose private customer information to a government entity only in response to 'an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena' served by the government entity.'" 196 F.R.D at 560.

The Court rejected the FTC's contention:

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

> the FTC's invitation to interpret the phrase ‘trial subpoena’ as encompassing a discovery subpoena duces tecum issued under Rule 45.” 196 F.R.D. at 561.

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

> “Apple would apparently have us declare an implicit exception for civil discovery subpoenas. But by enacting a number of quite particular exceptions to the rule of nondisclosure, Congress demonstrated that it knew quite well how to make exceptions to that rule. The treatment of rapidly developing new technologies profoundly affecting not only commerce but countless other aspects of individual and collective life is not a matter on which courts should lightly engraft exceptions to plain statutory language without a clear warrant to do so.”

The Pen Register Statute, 18 U.S.C. §§ 3121-3127, generally prohibits (except under specifically-defined oversight), the attachment of equipment that will record identities of persons communicating with a targeted individual. A "pen register" is defined as "a ***device*** or ***process*** which records or decodes dialing, ***routing***, addressing, or ***signaling*** information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication." 18 U.S.C. § 3127(3) (emphasis added). Similarly, a "trap and trace device" refers to "a ***device***

or process which captures the incoming electronic or other impulses which ***identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication***, provided, however, that such information shall not include the contents of any communication." 18 U.S.C. § 3127(4) (emphasis added).

> "There can be no doubt that the expanded definition of a pen register, especially the use of the term 'device or process', encompasses e-mail communications and communications over the internet. In other words, internet service providers can use a 'process' which '. . . records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted.' Similarly, internet service providers can use a 'process' which '. . . captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing and signaling information reasonably likely to identify the source of a wire or electronic communication.'

In Re Application of the United States of America for an Order Authorizing The Use of a Pen Register And Trap On [xxx] Internet Service Account/User Name [xxxxxxxx@xxx.com], 396 F. Supp. 2d 45, 47 (D. Mass. 2005). The Court allowed the devices to be installed, but took care to enforce the rule that "the information shall not include the contents of any communication" as required by 18 U.S.C. §§ 3127(3) and 3127(4), quoted above.

> "An obvious problem occurs when one considers e-mail. That portion of the 'header' which contains the information placed in the header which reveals the e-mail addresses of the persons to whom the e-mail is sent, from whom the e-mail is sent and the e-mail address(es) of any person(s) 'cc'd' on the e-mail would certainly be obtainable using a pen register and/or a trap and trace device. However, the information contained in the

> ‘subject’ would reveal the contents of the communication and would not be properly disclosed pursuant to a pen register or trap and trace device. After all, '“contents”, when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport or meaning of that communication.’ Title 18 U.S.C. § 2510(8).” *Id*., at 48, footnote omitted.

The Court further addressed the issue:

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

> order to obtain certain information within the site. While this may be said to be "dialing, routing, addressing and signaling information," it also is "contents" of a communication not subject to disclosure to the government under an order authorizing a pen register or a trap and trace device.
>
> Second, there is the issue of search terms. A user may visit the Google site. Presumably the pen register would capture the IP address for that site. However, if the user then enters a search phrase, that search phrase would appear in the URL after the first forward slash. This would reveal content -- that is, it would reveal, in the words of the statute, ". . . information concerning the substance, purport or meaning of that communication." Title18 U.S.C. § 2510(8). The "substance" and "meaning" of the communication is that the user is conducting a search for information on a particular topic.
>
> 396 F.Supp.2d at 48-49.
>
> Accordingly, the Court ordered:
>
> "The disclosure of the 'contents' of communications is prohibited pursuant to this Order even if what is disclosed is also 'dialing, routing, addressing and signaling information.'
>
> "Therefore, the term 'contents' of communications includes subject lines, application commands, search queries, requested file names, and file paths"
>
> *Id*. at 50.

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

In other words, suppose a criminal investigation were to be directed at an online provider and a government attorney were to request a Court Order for the installation of a "pen register" at the provider's ISP, recording and storing the "server log data" requested here by plaintiffs. Such a Court Order could go so far as to order the recording of IP addresses of those who communicated with the provider but not the contents of the communications. The word "contents" should, on the foregoing authority, be construed so as to include the name of the .torrent file downloaded or uploaded or search terms related thereto. Hence, the Pen Register Act would prohibit disclosure of both the IP Address of a visitor to a website coupled with identification of any .torrent file uploaded or downloaded (as requested by plaintiffs) or the search terms entered by the visitor.

All of the foregoing Acts recognize the central and privileged place occupied by the online service provider. Necessarily, the provider must have access to the protected information for the purposes intended by the user or customer. Providers also make additional uses of such information. Consequently, the providers cannot be held liable under the Acts so long as they conform to certain legal requirements. *In re DoubleClick Inc. Privacy Litig*., 154 F. Supp. 2d 497 (S.D.N.Y. 2001); *In re Toys R Us, Inc., Privacy Litigation*, MDL No. M-00-1381 MMC, Master File No. C 00-2746 MMC, 2001 U.S. Dist. LEXIS 16947 (N.D. Cal. 2001); *Bohach v. City of Reno*, 932 F. Supp. 1232 (D. Nev. 1996); *Konop*, supra; *Quon v. Arch Wireless Operating Co., Inc*, 309 F. Supp. 2d 1204 (C.D. Cal. 2004).

Accordingly, the providers themselves are provided with exceptions for application of the Acts. Section 2511(2)(a)(i) exclupates:

> "an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service."

Under 18 U.S.C. § 2701(c)(1), the prohibitions against unlawful access to stored communications do not apply to conduct of or authorized by “a person or entity providing a[n] ... electronic communications service.” See also 18 U.S.C. § 2510(15) (“ ‘electronic communication service’ means any service which provides to users thereof the ability to send or receive wire or electronic communications,” exactly the acts defendants are charged with).

The ECPA would be turned on its head if express protections for providers of online services, like defendants, were to be disregarded.

Please note that 18 U.S.C. § 2510 (17) defines "electronic storage" as:

"(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
(B) any storage of such communication by an electronic communication service for the purpose of backup protection of such communication."

See *In re DoubleClick Inc. Privacy Litig*., 154 F. Supp. 2d 497, 511 (S.D.N.Y. 2001).

We note that such a definition is not congruent with the purposes and needs of Fed.R.Civ.Pro. 34 so as to provide a definition of “electronically stored information” as used in the Rule. Such a definition would put an impossible burden on service providers. The ECPA would again be turned on its head if its expansive definition of “electronic storage” meant to protect privacy were to be used to invade privacy as plaintiffs are seeking. The Advisory Committee overseeing amendments to Rule 34 had good reasons to disregard the definition of electronic storage in the SCA and to define standards set forth expressly in the Notes to the Rule.

III. Conclusion

For the foregoing reasons, defendants respectfully request that the Court deny Plaintiffs’ Motion for an Order Requiring Defendants to Preserve and Produce Certain Server Log Data etc. and each part of said Motion.

Dated: March 27, 2007

Respectfully submitted,

ROTHKEN LAW FIRM, LLP

By: ____________________

Ira P. Rothken, Esq.
Attorney for Defendants

PROOF OF SERVICE

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

On March 27, 2007, I served the within:

DEFENDANTS' FURTHER AND SUPPLEMENTAL MEMORANDUM OF POINTS AND AUTHORITIES IN OPPOSITION TO PLAINTIFFS' MOTION FOR AN ORDER (1) REQUIRING DEFENDANTS TO PRESERVE AND PRODUCE CERTAIN SERVER LOG DATA, AND (2) FOR EVIDENTIARY SANCTIONS AND IN SUPPORT OF DEFENDANTS' REQUEST FOR MONETARY SANCTIONS

By EMAIL and FEDEX by depositing a copy in an envelope, postage prepaid in a FEDEX BOX addressed as follows:

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

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct. Executed on March 27, 2007.

Jared R Smith