GAUNTLETT & ASSOCIATES
David A. Gauntlett (SBN 96399)
James A. Lowe (SBN 214383)
Brian S. Edwards (SBN 166258)
18400 Von Karman, Suite 300
Irvine, California 92612
Telephone: (949) 553-1010
Facsimile: (949) 553-2050
jal@gauntlettlaw.com
bse@gauntlettlaw.com

Attorneys for Defendants
Akanoc Solutions, Inc.,
Managed Solutions Group, Inc.
and Steven Chen

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA, SAN JOSE DIVISION

LOUIS VUITTON MALLETIER, S.A., Plaintiff, vs. AKANOC SOLUTIONS, INC., et al., Defendants.	Case No.: C 07-3952 JW Hon. Magistrate Judge Howard R. Lloyd **MEMORANDUM OF POINTS AND AUTHORITIES IN OPPOSITION TO MOTION TO COMPEL PRODUCTION OF ELECTRONIC COMMUNICATIONS CONTAINED ON INTERNET SERVERS** Date: April 29, 2008 Time: 10:00 a.m. Dept.: Courtroom 2, 5th Floor

Defendants Managed Solutions Group, Inc., ("MSG") Akanoc Solutions, Inc. ("Akanoc") and Steve Chen ("Defendants") submit the following memorandum of points and authorities in opposition to Plaintiff Louis Vuitton Malletier, S.A.'s ("LV") Motion to Compel Production of Data on MSG and Akanoc's Internet servers:

I. INTRODUCTION

Defendants Managed Solutions Group, Inc. ("MSG") and Akanoc Solutions, Inc. ("Akanoc") are Internet hosting companies based in Fremont, California. They rent IP addresses and Internet bandwidth, using approximately 1,500 computer servers to numerous third party resellers and other Internet hosting companies, who in turn host probably tens of thousands of individual Websites. A single IP address can be used by a single Website or it can be used by tens or hundreds or even thousands of Websites. The Defendants do not control or know what specific use is made of each IP address rented to others because they provide unmanaged IP addresses and servers. MSG and Akanoc only authorize a client, normally a web hosting reseller, to use one or more of its Internet servers, and one or more IP addresses on a monthly basis. MSG and Akanoc provide servers with standard hosting application software installed and give password control of the server to their customers for a minimal monthly charge.

Because MSG's and Akanoc's Internet servers are physically located in San Jose, California at the main U.S. west coast gateway to the Internet, their services are sought after by many companies needing Internet access for telephone services, for downloading large digital files on demand, for reselling Web hosting services to end users, etc. MSG and Akanoc are Internet Service Providers (ISPs) that provide transmission, routing, and connection for digital online communication for their customers but have no role in choosing, authorizing, modifying or monitoring the information stored or transmitted.

As with all Internet service providers,[1] a small fraction of the Websites hosted by their

[1] *See* 17 U.S.C. 512(k)(1)(A) that defines [Internet] service provider as "... an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received."

customers may from time to time contain objectionable content, including possibly offering counterfeit goods for sale. MSG and Akanoc have no relationship, either directly or indirectly, with any of the operators of Websites hosted on their servers. They simply provide access to the Internet and have no knowledge of the contents of Websites being hosted on their servers unless a specific complaint is brought to their attention. Only then can they check to see if a specific offending Website is using one of their servers. Prior to that time the Defendants do not have any information about allegedly objectionable content stored on their servers.

Plaintiff LV makes and markets handbags and other merchandise worldwide, including in California, and maintains a manufacturing plant in San Dimas, California. LV brought the instant action against MSG, Akanoc, and the principal of both companies, Steven Chen, seeking monetary damages for contributory and vicarious trademark and copyright infringement. LV's apparent theory is that MSG and Akanoc are liable because Websites that offered allegedly counterfeit LV products for sale were hosted on their servers.

LV seeks production of *all* of the third party content contained on servers owned by Defendants ("publicly posted Internet content" and "traffic logs", LV P&A, 4:3-8). The requested production encompasses the content of an unknown number of Websites but could easily exceed millions of Websites.[2] But LV's investigator testified at his deposition on April 1, 2008 that he has only investigated between 5 and 15 Websites hosted on MSG and Akanoc's servers in connection with this case.[3] So of all Websites LV is seeking to compel, inspection of at most only 15 are potentially at issue.

---

[2] Together MSG and Akanoc have assigned to them approximately 30,000 IP addresses. Each IP address can be used by multiple Websites at the discretion of the customer to whom these Defendants "rent" monthly authorization to use IP addresses. Each IP address can be used by a minimum of one Website, but can be used by ten or hundreds or even thousands of Websites. If an average of ten Websites used each rented IP address, there could be 300,000 Websites using Defendants' servers. But if each IP address was used by 1000 Websites then up to three million Websites could be hosted on the Defendants' 1,500 servers. The Defendants do not control and do not know how many Websites use its servers at any given time but the number is expected to be very large.

[3] The appropriate excerpts from Mr. Holmes' deposition transcript are attached to the Declaration of James Lowe filed herewith.

But more importantly, disclosing the contents of any of the server content is specifically prohibited by federal criminal law. Doing so would subject MSG and Akanoc to civil and criminal liability. LV seems ignorant of this fact. LV cites no statutes, case law or other legal authority that allows LV access to the content of MSG's and Akanoc's servers. No law authorizes this Court to permit access in this case.

II. IT IS A VIOLATION OF FEDERAL LAW FOR DEFENDANTS TO DISCLOSE THE CONTENTS OF THEIR SERVERS TO LOUIS VUITTON

A. Defendants Are Subject to Criminal Penalties if They Disclose the Contents of Electronic Communications on Their Servers

The Wiretap Act (18 U.S.C. 2510 et seq.) specifically prohibits the interception and monitoring of electronic communications such as the contents of MSG's and Akanoc's servers.

18 U.S.C. 2511(1)(a) provides as follows:

> Except as otherwise specifically provided in this chapter any person who—
>
> (a) intentionally intercepts. . .any wire, oral or electronic communication;
>
> * * *
>
> (c) intentionally discloses…to any other person the contents of any wire, oral or electronic communication, knowing or having reason to know the information was obtained through the interception of a wire, oral or electronic communication in violation of this subsection
>
> * * *
>
> shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

Violation can result in criminal penalties. Subsection (4)(a) of Section 2511 provides that "…whoever violates subsection (1) of this section shall be fined under this title **or imprisoned not more than five years**, or both."

It is also unlawful to monitor the content of electronic communications on MSG's and Akanoc's servers.

/ / /

18 U.S.C. 2511(2)(a)(i) provides as follows:

...[A] provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

B. The Stored Communications Act (18 U.S.C. § 2700, et al) Prohibits Disclosure of Content Stored on Defendants' Servers

In 1996, Congress passed the Electronic Communications Privacy Act ("ECPA") in order "to ensure the security of electronic communications." *Quon v. Arch Wireless Operating Co., Inc.*, 309 F.Supp.2d 1204, 1207 (C.D.Cal. 2004) Title II of the ECPA created the Stored Communications Act ("SCA").[4] The SCA addressed "access to stored wire and electronic communication and transactional records." *Quon v. Arch Wireless Operating Co., Inc.,* 309 F.Supp.2d at 1207, citing to S.Rep. No. 99-541, at 3; 1986 U.S.C.C.A.N at 3557. "The ECPA's legislative history indicates that Congress passed the SCA to prohibit a provider of an electronic communications service 'from knowingly divulging the contents of any communication while in electronic storage by that service to any person other than the addressee or intended recipient.'" *Quon v. Arch Wireless Operating Co., Inc.*, 309 F.Supp.2d at 1207, citing to S.Rep. No. 99-541, at 37; 1986 U.S.C.C.A.N at 3591.

Section 2702(a)(1) of the SCA specifically prohibits disclosure of the content of communications in electronic storage:

> A person or entity providing an electronic communication[5] service to the public **shall not** knowingly **divulge** to any person or entity the **contents** of a **communication** while **in electronic storage** by that service.

18 U.S.C. § 2702(a)(1) (emphasis added)

The SCA defines an "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Courts have interpreted this language to apply to Internet service providers like Akanoc

---

[4] Title I of the ECPA amended the Wiretap Act to adopt for the SCA the same definitions as used in the federal Wiretap Act. *See* 18 U.S.C. § 2711

[5] An "electronic communication" is defined as: any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce..." 18 U.S.C. § 2510(12).

and MSG: "The ECPA definition of 'electronic communications service' clearly includes Internet service providers such as America Online, as well as telecommunications companies whose cables and phone lines carry internet traffic." *Dyer v. Northwest Airlines Corporations,* 334 F.Supp.2d 1196, 1199 (D.N.D. 2004) Since Akanoc and MSG are Internet service providers (whose servers and routers carry Internet traffic and provide access to the Internet including the ability to send and receive electronic communications) they are covered governed by the SCA.

As shown above, Section 2702 bars disclosure of communications in "electronic storage" on MSG and Akanoc's servers. The term "electronic storage" in Section 2702 is defined broadly as follows:

> (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 purposes of backup protection of such communication. [6]

18 U.S.C. § 2510(17).

Courts have acknowledged that Websites are in "electronic storage" for purposes of the SCA. See *Konop v. Hawaiian Airlines, Inc.,* 302 F.3d 868, 879 (9th Cir. (Cal.) 2002) ("The parties agree that the relevant 'electronic communications service' is Konop's Website, and that the website was in 'electronic storage.'")

C. Disclosure Would Subject Defendants to Significant Civil Liability

Disclosing the contents of the Internet servers would subject MSG and Akanoc to significant civil liability. Section 2707(a) of the SCA (18 U.S.C. § 2707) provides a private right of action against Akanoc and MSG should they disclose the content of their servers:

> "[A]ny… subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the…entity…which engaged in that violation such relief as may be appropriate."

A party 'knowingly' discloses protected information if it is aware of the disclosure and does not do so inadvertently. See *Freedman v. America Online, Inc.,* 329 F.Supp.2d 745, 749 (E.D.Va.

[6] Either part of the definition of "electronic storage" is sufficient under the SCA. *Quon,* 309 F.Supp.2d at 1207, citing to S.Rep. No. 99-541, at 35; 1986 U.S.C.C.A.N at 3590.

2004) ("Plaintiff has shown that Sheridan "knowingly divulge[d]" Plaintiff's subscriber information. Sheridan was undoubtedly aware of the disclosure; she did not disclose the information inadvertently.")

For each customer whose content is produced to LV, a court can assess actual damages of at least $1,000.00 and attorneys fees and costs. If the violation is willful or intentional the court can assess punitive damages. 18 U.S.C. § 2707(b) Disclosure of content is considered intentional if it is not done inadvertently. No *mens rea* or specific intent to violate the statute is required: "Legislative history and authority interpreting Title I of the ECPA point persuasively to the conclusion that an ISP acts intentionally provided only that its acts are not inadvertent." See *Freedman,* 325 F.Supp.2d at 751.

Given the huge number of Websites at issue (50,000), civil damages against Akanoc and MSG could total in the tens of millions of dollars.

D. There is No "Civil Discovery" Exception to the SCA

None of the eight narrow exceptions to the SCA set forth at 18 U.S.C. 2702(b) apply.[7]

---

[7] Section 2702(b) sets forth the following exceptions:

A provider described in subsection (a) may divulge the contents of a communication--

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032);

(7) to a law enforcement agency--

(A) if the contents--

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

In the context of civil discovery Courts interpret the provisions of the SCA narrowly against disclosure of electronic communications. An example is *F.T.C. v. Netscape Communications Corp.* 196 F.R.D. 559, 561 (N.D.Cal.2000). In that case the Court interpreted Section 2703(c)(1)(C) of the SCA which allows disclosure of private customer information pursuant to a "trial subpoena" issued by a government agency. The issue was whether a civil discovery subpoena issued during the pre-trial discovery phase of the underlying civil action constituted a "trial subpoena" as contemplated by Section 2703(c)(1)(C). Id. at 560 In refusing to interpret the term "trial subpoena" to include a pre-trial civil discovery subpoena, the court stated: "There is no reason for the court to believe that Congress could not have specifically included discovery subpoenas in the statute had it meant to." Id. at 561

State courts are also loathe to find exceptions to the SCA for civil discovery. In *O'Grady v. Superior Court (Apple Computers, Inc.)*, 139 Cal.App.4th 1423, 1442-43 (Cal.App.6th Dist 2006) Apple Computers, Inc. sued Web site publishers alleging they had published confidential company information about an impending product, and sought to identify the source at Apple of the disclosures. In quashing Apple's civil subpoenas, the court found that the information requested in the subpoenas were covered by the SCA. *Id.* at 1480 In rejecting Apple's argument "that Congress did not intend to 'preempt' civil discovery of stored communications, and the Act should not be given that effect," the court held as follows:

> Apple would apparently have us declare an implicit exception [to the SCA] for civil discovery subpoenas. But by enacting a number of quite particular exceptions to the rule of non-disclosure, 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. We should instead stand aside and let the representative branch of government do its job.

O'Grady v. Superior Court (Apple Computers, Inc.), 139 Cal.App.4th at 1443.

---

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

III. LV CITES TO NO AUTHORITY THAT ALLOWS DISCLOSURE OF CONTENT STORED ON INTERNET SERVERS

At page 8 of its brief, LV cites *In re Verizon Internet Services, Inc.*, 257 F. Supp.2d 244 (D.D.C. 2003) for the proposition that an Internet Service Provider may be compelled to produce electronic records stored on its servers. However, that case is not applicable on its facts. Verizon brought a motion to quash a subpoena issued by the Recording Industry Association of America ("RIAA") for the **identity** of an anonymous user of the conduit functions of Verizon's Internet service alleged to have infringed copyrights by offering hundreds of songs for downloading over the Internet. Id. at 246. The subpoena was issued by the RIAA pursuant to Section 512(h) of the Digital Millennium Copyright Act (17 U.S.C. § 512). *Id.* at 246.

Section 512(h) states, in pertinent part, as follows:

> h) Subpoena to identify infringer.--
>
> A copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection.

This case therefore has no application to the instant motion as LV is seeking to compel the content of Akanoc and MSG's servers (which disclosure is prohibited by 18 U.S.C. § 2702(a)(1)), and not the identity of any alleged infringers. Defendants have already produced detailed records to LV in discovery that disclose the identity of all of Akanoc's and MSG's past and current customers.

LV's brief, at page 8, cites *Playboy Enterprises, Inc. v. Welles,* 60 F.Supp.2d 1050 (S.D. Cal. 1999) for its contention that Akanoc and MSG's servers must be made available for inspection. That case however concerned only whether Playboy was entitled to access the Defendant's **own computer hard drive** to attempt to recover Defendant's deleted e-mails. *Id.* at 1051. *Playboy* is inapposite for the obvious reason that disclosure of Akanoc's and MSG's own computer hard drives is not at issue. MSG and Akanoc have already provided content of its own e-maiil server and allowed the Plaintiff to copy the hard drive of their e-mail server for further examination. Whether the content of Internet servers could be disclosed was not an issue in *Playboy* and that case is therefore not relevant to the instant motion.

LV also cites *In re Banker's Trust,* 61 F.3d 465 (6th Cir. 1995) for its contention that MSG's

and Akanoc's alleged 'control' over electronic data on its servers is sufficient to mandate production. (Coombs Dec., ¶5) But that case has nothing to do with production of electronic data in discovery. The issue there was whether the 'bank examination privilege' applies to bar disclosure of documents prepared by the Federal Reserve during a bank examination. *Id.* at 469. LV fails to discuss the case or otherwise elaborate on how it could possibly be analogous or applicable to the instant motion.

IV. DEFENDANTS DID OBJECT TO LV'S DOCUMENT REQUESTS AND HAVE NOT WAIVED ANY OBJECTIONS

At Section B of its brief, LV sets forth the document production requests it is seeking to compel. However, in violation of Local Rule 37-2[8], LV failed to set forth Defendants objections to the requests, instead incorrectly informing the Court that: "Defendants do not object to production and have waived any objections concerning the cost or burden of such a production, any otherwise applicable privileges or that the requests are in some manner overbroad." (LV P&A, p.7:25-28) Nothing could be further from the truth.

Defendants did object to all of LV's requests on numerous basis, among them attorney client privilege, attorney work product, that the requests are vague, ambiguous and overly broad as to the term "Internet Content," and that the requests are overly broad and unduly burdensome as to the unspecified time period.

MSG and Akanoc also objected to each of LV's requests "to the extent they call **for information protected by** the United States Constitution, the California Constitution, and **any applicable statutes**, including the right of privacy." (emphasis added) Thus, contrary to LV's incorrect representations, Defendants served appropriate objections and have not waived them. True copies of MSG's and Akanoc's responses to LV's Request for Production of Documents, Set Two, are attached as exhibits to the accompanying Declaration of James Lowe.

///

[8] Local Rule 37-2 states in pertinent part: "In addition to complying with applicable provisions of Civil L.R. 7, a motion to compel further responses to discovery requests must set forth each request in full, **followed immediately by the objections** and/or responses thereto." (emphasis added)

V. CONCLUSION

For the above reasons, Defendants Managed Solutions Group, Inc., Akanoc Solutions, Inc. and Steven Chen respectfully requests that Plaintiff Louis Vuitton Malletier, S.A.'s instant motion to compel be denied in its entirety.

Dated: April 8, 2008

GAUNTLETT & ASSOCIATES

By: s/James A. Lowe
James A. Lowe
Brian S. Edwards

Attorneys for Defendants
Akanoc Solutions, Inc.,
Managed Solutions Group, Inc.,
and Steven Chen