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 (HRL) Hon. James Ware **DEFENDANTS' OBJECTION TO ORDER GRANTING PLAINTIFF'S MOTION TO COMPEL PRODUCTION OF DOCUMENTS**

TABLE OF CONTENTS

Defendants Managed Solutions Group, Akanoc Solutions, Inc. and Steve Chen hereby object to the Magistrate Judge's Order Granting Plaintiff's Motion to Compel Production of Documents.

Under Fed. R. Civ. P. 72(a), a district judge in the case must consider timely objections and modify or set aside any part of the order that is clearly erroneous or is contrary to law." The Magistrate Judge's order is "clearly erroneous" and contrary to law because it requires Defendants to hack into Internet servers containing its customers' private information, thereby violating federal criminal law. The Magistrate Judge's order should be set aside.

I. THE DISCOVERY ORDER IS CLEARLY ERRONEOUS BECAUSE IT REQUIRES DEFENDANTS TO VIOLATE FEDERAL STATUTES

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

Defendants Managed Solutions Group, Inc. and Akanoc Solutions, Inc. (collectively "MSG") are Internet service providers that use approximately 1,500 computer servers in San Jose, approximately 40,000 Internet Protocol ("IP") addresses assigned to them and substantial Internet bandwidth purchased from wholesale communications providers to provide Internet service packages to its customers. These packages, which consist of a group of IP addresses, a specific quantity of Internet communication bandwidth and use of computer servers with hard drive storage space, are rented to customers, often international resellers of ISP services, for a fixed amount per month. The servers are provided with a basic operating system and software to access the Internet. Customers provide their own applications and content. MSG's packages are desirable because they enable access to main U.S. Internet "pipes" with high quality stable services. They are used by large scale customers with the technical ability to manage their operations remotely and without the need for heavily managed services. MSG offers, effectively, bare bones Internet access at low prices.

MSG does not know what any customer does with the ISP services unless a customer happens to tell them. Some ISP services and equipment are used for data storage, some for downloading software, some for interactive computer games, and some to operate websites. A given package including a server may be used for a single purpose or may be resold for use by multiple customers who are unknown to MSG. A single IP address can be used for hundreds or thousands of websites, for example, depending on the size of storage space used and the volume of traffic.

Upon payment of a monthly fee the customer is given exclusive access to the server controlled by a password selected by the customer. After the server access is turned over to a customer, MSG and their manager Steve Chen have no access to the servers and are prohibited by federal law from monitoring[1] any content transmitted or stored by the customers. The only exception is when a customer has technical problems it cannot solve and specifically requests some server maintenance by MSG personnel. On those occasions the customers must give MSG a password to access the server. When a computer server is no longer used by a customer (the rental agreement terminates), MSG still has no access to the hard drive content. MSG personnel simply reformat the hard drive(s), reinstall an operating system and rent the equipment to a new customer.

Plaintiff Louis Vuitton alleges contributory or vicarious trademark and copyright infringement alleged to arise from advertising of counterfeit Louis Vuitton merchandise on up to 67 websites alleged to be using ISP services sold by MSG's reseller customers. Louis Vuitton thinks it may find evidence about websites offering counterfeit merchandise if it can inspect the MSG servers. MSG was unable to provide information about anything that might or might not be stored on its servers and did not provide Louis Vuitton access to the servers because MSG has no access to the content of any servers. All servers are password protected by its customers in the normal course of its business. MSG has no legal right to access what is stored on the servers and MSG has no practical or technical ability to access any hard drive. MSG can only format (and erase) a server hard drive but cannot see any content on it. Louis Vuitton has never suggested how MSG could access any hard drive content, even if such access were not a criminal offense.

The Magistrate Judge's Order requires defendants to either (1) produce all responsive publicly posted Internet content evidencing offers made of counterfeit Louis Vuitton merchandise and traffic logs evidencing the volume of underlying counterfeit activity, or (2) permit inspection of their servers to allow plaintiff an opportunity to ascertain the same. Defendants would violate the federal Stored Communications Act ("SCA") by even attempting to comply with this order. The

[1] It is unlawful for Defendants to monitor the content of electronic communications on their servers under 18 U.S.C. 2511(2)(a)(i): "[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."

SCA prohibits Defendants from disclosing the contents of communications in electronic storage:

> A person or entity providing an electronic communication[2] 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.[3] (emphasis added)

The Defendants are subject to the SCA as electronic communication service providers defined by the SCA as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[4] MSG is governed by the SCA because they are Internet service providers whose servers, routers and cables carry Internet traffic and provide access to the Internet including the ability to send, receive and store electronic communications. *Dyer v. Northwest Airlines Corporations,* 334 F.Supp.2d 1196, 1199 (D.N.D. 2004) ("The . . .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.")

The website files ordered produced are "electronic storage" under the SCA. If the information sought by Louis Vuitton exists at all, it would only exist in electronic storage on the computer servers. The Ninth Circuit agrees that website information stored on a computer is "electronic storage" as defined by 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.'")

B. Complying With the Magistrate Judge's Order Would Subject Defendants to Criminal and Significant Civil Liability

1. Defendants' Criminal Liability Under the SCA

The Magistrate Judge's Order forces Defendants to subject themselves to criminal liability including fines and up to 10 years imprisonment.[5] Section 2701(a) of the SCA creates criminal

---

[2]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).

[3]18 U.S.C. § 2702(a)(1)

[4]18 U.S.C. § 2510(15).

[5]18 U.S.C. § 2701(b)

liability for obeying the Magistrate Judge's discovery order:

> Except as provided in subsection (c) of this section whoever—
> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
> (2) intentionally exceeds an authorization to access that facility;
> and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

Complying with the Magistrate Judge's order would subject Defendants s to criminal liability under the SCA because Defendants do not have authorization to access its customers' information on its servers. The discovery order cannot provide the requisite authorization.

The only person who can give "authorization" under the SCA is a "user" of the service.[6] A "user" is defined as one who uses the service and is duly authorized to do so.[7] Even being eligible to access a website or Internet service is not enough to qualify as a "user" under the SCA; one must have permission from the owner of the website and actually access the service in order to be able to give authorization under the SCA.[8] Under this strict definition, neither the Defendants nor the Magistrate Judge can give authorization under the SCA because they are not "users" under the SCA. The only "users" that can give authorization are the website owners. Defendants do not have, nor can they obtain, the authorization to comply with the Magistrate Judge's order. As discussed below, the discovery order cannot grant "authorization" for access. Defendants' will be subject to criminal liability by attempting to comply with the Magistrate Judge's order because they have no authorization from the users of the data stored on the servers.

2. Defendants' Civil Liability under the SCA

The Magistrate Judge's Order would also subject the Defendants to significant civil liability. The SCA provides a private right of action against the Defendants if they disclose the content of their servers:

> "[A]ny… subscriber, or other person aggrieved by any violation of this

[6] 18 U.S.C. § 2701(c)(2)

[7] *Id.*

[8] *Konop*, 302 F.3d at 880 (holding that even a Hawaiian Airlines employee who was merely authorized to access Snow's website, but had not actually accessed it himself, was (1) not a "user" under the SCA and (2) could not give authority under the SCA to Hawaiian Airlines to access Snow's website using the employee's name.)

> 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."[9]

MSG does not know the identity of all potential persons who would be aggrieved by violation of the SCA, none of these parties are before the court, none have been identified by Louis Vuitton, and the court has no power to immunize the Defendants against any liability.

Defendants would easily be found to have 'knowingly' disclosed protected information because a party 'knowingly' discloses protected information if it is aware of the disclosure and it is not inadvertent. *See Freedman v. America Online, Inc.*, 329 F.Supp.2d 745, 749 (E.D.Va. 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 Vuitton, 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.[10] Disclosing content is considered intentional if it is not done inadvertently. No *mens rea* or specific intent to violate the statute is required. *See Freedman*, 325 F.Supp.2d at 751.

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

Louis Vuitton's suggestion and the Magistrate Judge's apparent assumption is that a discovery order of this court is sufficient to get around the prohibitions of the SCA to access the servers. That idea is entirely mistaken. The SCA has no civil discovery exception.

A civil discovery subpoena does not create an exception to the SCA. In the context of civil discovery, courts interpret the provisions of the SCA narrowly against disclosure of electronic communications. In *F.T.C. v. Netscape Communications Corp.* 196 F.R.D. 559, 561 (N.D.Cal.2000), the court interpreted Section 2703(c)(1)(C) of the SCA that allows disclosing private customer information pursuant to a "trial subpoena" issued by a government agency. The issue was whether a

[9] 18 U.S.C. § 2707(a)

[10] 18 U.S.C. § 2707(b).

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."

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 website publishers alleging publication of confidential 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 was 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:

> 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.

Defendants cannot legally comply with the Magistrate Judge's order because none of the eight very narrow exceptions to the SCA set forth at 18 U.S.C. 2702(b) [11] applies here. Although an

[11] 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

ISP can provide access to stored communications pursuant to a search warrant and avoid liability under the SCA. But search warrants are not authorized for civil discovery. MSG periodically receives search warrants authorizing the FBI, CIA or Homeland Security to access and hack into hard drives on its servers for criminal or national security investigations. But otherwise it has not and cannot allow or obtain access.

D. The Material Ordered Produced is SCA-Protected Because It Is Configured to Limit Ready Access by the General Public

Contrary to the Magistrate Judge's Order, this material ordered produced (if it exists at all) is ***not* "configured to permit ready access by the general public"** and Defendants would violate the SCA by attempting to comply with the court's order.

1. The Configuration of the Material Sought

The Magistrate Judge's Order says that because the material Vuitton seeks is publicly accessible, it is not subject to SCA protection. But that conclusion is mistaken. The material ordered produced is SCA-protected because it is expressly configured **not** to be publically accessible. This material is (1) stored on Defendants' Internet servers located in Defendants' secured, publicly inaccessible, San Jose, California facility[12] and (2) only accessible by Defendants' own customers because only those individual customers have the passwords[13] to access the servers.[14]

---

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

(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.

[12]Declaration of Steve Chen in Opposition to Motion to Compel Production of Electronic Communications on Internet Servers ("Chen Decl.") ¶4.

[13]Chen Decl. ¶3

[14]The Magistrate Judge's Order states that "at the motion hearing, defendants also confirmed that

The Ninth Circuit has held that SCA protection applied to a website whose owner (a Hawaiian Airlines pilot) limited access to it by requiring users to input the names of Hawaiian Airlines pilots. *Konop*, 302 F.3d at 879-881. In that situation, access to the website by Hawaiian Airlines executives was found improper even when "authorized" by pilots who permitted their supervisors to use their identity to gain access to an anti-company site. *Snow v. DirecTV*, 450 F.3d 1314, 1322 (11th Cir. 2006) agreed that the *Konop* website was SCA-protected because its modest access restriction was sufficient to limit ready access by the general public.

Vuitton argued that because the websites it accuses of selling counterfeit merchandise are accessible to the public through an Internet browser and the World Wide Web, that hacking into servers that might store images shown on the World Wide Web should be seen as readily accessible by the general public. But if this material stored on Defendants' servers was readily accessible by the general public, Vuitton would not need an order compelling discovery to obtain it. Obviously what is available to the general public about the accused websites on the World Wide Web is not sufficient for Vuitton's purposes; it wants non-public information. Even if Vuitton could clearly identify which of the 1,500 servers any one of the 67 websites might have used, the idea that there is ready public access to the servers is nonsensical. It is equivalent to a burglar arguing that because a retail store is open to the public, that breaking into the back door and inspecting property in the manager's safe is equally authorized.

The Magistrate Judge's Order forces Defendants to attempt to produce material whose public access is even more restricted than the material in *Konop*. This material is clearly protected by the SCA because it is "configured in some way so as to limit ready access by the general public" (with a customer's secret password) and Defendants cannot legally attempt to produce this material.

---

their servers rotate in and out of use, that defendants initially assign passwords to their clients, and that defendants also re-set passwords when servers have been "returned" or "abandoned." (Order Granting Plaintiff's Motion to Compel Documents, fn 4, p.4) While this is true, the Magistrate Judge's order fails to mention that, while defendants do reset passwords when they reformat the hard drive and reconfigure returned or abandoned servers the passwords are then changed by customers once the servers are put back into use. Once the customers change the passwords, defendants are unable to access the server using the old password. [Chen Decl. ¶3].

2. Traffic Logs

The Magistrate Judge's Order also mandates that Defendants produce "traffic logs evidencing the volume of underlying counterfeit activity." Defendants have no basis for ascertaining what types of logs would satisfy this order. Vuitton has never identified the type of traffic logs it seeks and no evidence shows the defendants keep or that their customers keep logs that would satisfy this portion of the order. But even if any such traffic logs exist on Defendants' servers, they too would not be "configured for public access" and cannot be produced under the SCA.

II. COMPLYING WITH THE MAGISTRATE JUDGE'S ORDER WOULD BE IMPOSSIBLE, SHOWING IT TO BE CLEARLY ERRONEOUS

The Magistrate Judge's Order supposedly limits the scope of the discovery inspection to 67 websites, but this does not make compliance with the order possible; it is not as if there are sixty-seven discrete places to look (even assuming the technical ability and the legal right to do so). The Defendants do not believe any of the sixty-seven websites are using its servers at all and certainly do not know where to look for them. Louis Vuitton has not provided evidence to the court and the order does not identify any specific places to search. Indeed, Louis Vuitton does not know the identity of any operator of any allegedly infringing website.

Defendants have approximately 1,500 computer servers that store data for thousands of customers worldwide. Regardless of the number of websites Louis Vuitton wants evidence about, any attempts to comply with the Magistrate Judge's order would require Defendants to somehow search through all the data on all 1,500 of its servers looking for traces of evidence about 67 websites that may or may not have used the servers in the past. Whether Defendants search for one needle or sixty-seven needles, the search would involve searching not one but 1,500 haystacks. This task would be nearly impossible, and Vuitton has never offered a suggestion as to how this task may be feasibly completed, technically or practically.

Any such searches would necessarily disrupt services to all customers using MSG servers, creating additional liability that would threaten the very business of the Defendants. This order is akin to a discovery order to an owner of 1,500 apartment units where the owner is required to break into each unit and plunder through the private papers of every renter in order to allow a plaintiff to

see if there might be evidence that sixty-seven individuals had ever been in the apartments or sold allegedly infringing handbags.

The entire idea is absurd. Even if such a search were practical, even if it did not violate federal criminal law, even if it would not harm thousands of entirely innocent persons, even if it did not create unending civil liability for the Defendants, and even if it did not violate the Fourth Amendment, an order for such a search is outrageous and clearly erroneous.

Both the Magistrate Judge's order and the Supplemental Declaration of J. Andrew Coombs ("Coombs Decl.") simply assert that the Defendants have the technological ability to perform searches on its servers Defendants' entirely theoretical technological ability to search their servers does not make compliance with the Magistrate Judge's Order easier. For instance, paragraphs 5 and 6 of the Coombs Decl. state that Defendants may use search terms to search content on its servers. Vuitton has never provided any direction on what search terms Defendants could use to definitively identify the material that Vuitton seeks. Even searching all 1,500 servers for just the names of the 67 websites would require performing over 100,000 searches. But this argument falsely assumes (without a shred of evidence) that the Defendants have actual access to the servers. The searches suggested by Louis Vuitton would first require hacking into each and every server to be "inspected." The Defendants are not in the business of computer hacking and do not intend to learn that trade. At best, Louis Vuitton would need to employ persons skilled in computer crime. The Magistrate Judge's Order is not feasible legally nor is it feasible technologically. It is clearly erroneous.

III. CONCLUSION

Louis Vuitton misled the Magistrate Judge to issue a discovery order that is entirely impractical, that violates federal criminal law, that exceeds the relief available under the discovery rules, and that is clearly erroneous. This order should be set aside.

Dated: July 25, 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 Steve Chen