Hanni M. Fakhoury (SBN 252629)
hanni@eff.org
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Attorneys for Amicus Curiae
ELECTRONIC FRONTIER FOUNDATION

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

ROYBAL DIVISION

CHLOE SAS, *et al*.,

Plaintiffs,

v.

SAWABEH INFORMATION SERVICES CO., *et al*.

Defendants.

SAWABEH INFORMATION SERVICES CO., a Saudi Arabian Corporation; TRADEKEY (PVT) LTD, a Pakistani Corporation,

Counterclaimants,

v.

RICHEMONT INTERNATIONAL LIMITED, *et al*.

Counterclaim Defendants.

Case No. 2:11-cv-04147-GAF-MAN

BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF COUNTERCLAIMANTS OPPOSITION TO MOTION TO DISMISS COUNTERCLAIMS

Courtroom: 740
Judge: The Hon. Gary A. Feess

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

RULES

LEGISLATIVE MATERIALS

INTRODUCTION

This case presents a dilemma of modern litigation: how do courts reconcile a civil litigant's need to stop a perceived legal and financial harm in a way that does not intrude on the privacy of scores of innocent people who have nothing to do with the dispute in the first place?

The Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-2712, expressly prohibits private civil litigants from obtaining the contents of electronic communication records from communication providers. Although government entities have limited access to this information, the fact that private litigants do not is no accident. Rather, it reflects Congress' purpose in enacting the SCA: "to protect internet subscribers from having their personal information wrongfully used and publicly disclosed by '*unauthorized private parties*.'" *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp. 2d 606, 610 (E.D. Va. 2008) (quoting S. Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557) (emphasis added).

The seizure that occurred here thwarts that purpose. In one fell swoop, counterclaim defendants accessed 9 million emails and 71,000 stored chats, the majority of which had nothing to do with the trademark infringement dispute that prompted the seizure. Second Amended Counterclaim ("SACC") ¶¶ 48, 66.[1] Yet, in

[1] As the court must in assessing a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6), amicus assume all facts in the counterclaim to be true. *See Sprewell v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001) ("All *(footnote continued on following page)*

urging dismissal of the counterclaims, counterclaim defendants assert the Lanham Act's seizure provision in 15 U.S.C. § 1116(d) renders the SCA's privacy protections irrelevant and permits access to stored electronic communications held by a communications provider with no restrictions whatsoever. Not even law enforcement has the sweeping powers that counterclaim defendants now imply belong to intellectual property litigants.

Moreover, since a Lanham Act seizure is not specifically listed in the exceptions to the SCA's prohibition of private civil litigants' access to the content of communications, accepting counterclaim defendants' rationale would make the vast amounts of electronic content stored by a communications provider available to *all* civil litigants, regardless of its relevance to the legal dispute at issue and without any restriction.

Because this unprecedented expansion of the Lanham Act contradicts Congress' clear intent to protect the contents of electronic communications from the hands of private parties and civil litigants, this Court should deny the motion to dismiss the counterclaims.

ARGUMENT

The plain text of the SCA prohibits a communications provider from disclosing the contents of electronic communications to civil litigants. While there

---

(footnote continued from preceding page)
allegations of material fact are taken as true and construed in the light most favorable to the nonmoving party.").

are exceptions to this broad prohibition, none of them apply to civil litigants generally, or to Lanham Act seizures specifically. In the absence of any statutory exception to the SCA's prohibition in accessing content, a Lanham Act seizure order cannot provide the "authorization" necessary to permit disclosure of content under the SCA. Nor did the May 2011 seizure order permit the seizure of the contents of communications because by ordering a seizure prohibited by the SCA, the order was invalid, and any resulting access unauthorized. The Lanham Act can coexist with the SCA by permitting courts to authorize the seizure of electronic data from communications providers within the boundaries of the SCA. Noncontent records stored by electronic communications providers are accessible, and Lanham Act litigants can apply for and obtain seizure orders directing providers to disclose this material. But what civil litigants cannot do is what happened here: apply for and obtain permission to seize the content of stored electronic communications. As a result, the motion to dismiss the counterclaims should be denied.

A. The Stored Communications Act Prohibits Civil Litigants, Including those with Lanham Act Seizure Orders, From Accessing Electronic Communications Stored By Communications Providers.

The SCA prohibits accessing and obtaining the contents of electronic communications stored by a communications provider subject only to a limited set of enumerated exceptions. None of these exceptions applies to civil litigants, regardless of the Lanham Act's seizure authority in 15 U.S.C. § 1116(d).

1. The Plain Text of the SCA Prohibits Civil Litigants From Accessing the Contents of Communications.

When a "statute's language is plain, 'the sole function of the courts is to enforce it according to its terms.'" *United States v. Ron Pair Enterprises, Inc.*, 489 U.S. 235, 241 (1989) (quoting *Caminetti v. United States*, 242 U.S. 470, 485 (1917)). The court's "first step" is "to determine whether the language at issue has a plain and unambiguous meaning" and a court's inquiry must end "if the statutory language is unambiguous and 'the statutory scheme is coherent and consistent.'" *Robinson v. Shell Oil Co.*, 519 U.S. 337, 340 (1997) (quoting *Ron Pair Enterprises, Inc.*, 489 U.S. at 240). "The plainness or ambiguity of statutory language is determined by reference to the language itself, the specific context in which that language is used, and the broader context of the statute as a whole." *Robinson*, 519 U.S. at 341. The plain text of the SCA demonstrates that civil litigants are not permitted to obtain the contents of electronic communications from providers.

The SCA criminalizes anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided" or "intentionally exceeds an authorization to access that facility." 18 U.S.C. § 2701(a)(1), (2).[2] There are few enumerated exceptions to this broad prohibition, none of which applies to private litigants.

[2] An "electronic communication service" ("ECS") is "any service which provides to users thereof the ability to send or receive wire or electronic communications." *(footnote continued on following page)*

As the legislative history makes clear, the SCA was intended to "protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs." S. Rep. No. 99-541, at 3, 1986 U.S.C.C.A.N. at 3557. Thus, 18 U.S.C. § 2703 provides the mechanism by which law enforcement can compel access to the content of stored electronic communications from communication providers. 18 U.S.C. § 2703(a)-(d). And in 18 U.S.C. § 2702(b), providers of communication services may voluntarily disclose content to law enforcement in cases of dangerous emergencies or if the provider discovers evidence relating to a crime, including child pornography. 18 U.S.C. § 2702(b)(2), (6)-(8); *see generally* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1221-22 (2004).[3]

Other than obtaining the consent of the user whose communication is at issue, the SCA provides no mechanism for private litigants to obtain content from a provider of communication services. *See* 18 U.S.C. §§ 2701(c)(2), 2702(b)(3). The SCA contains no explicit exception for Lanham Act seizures specifically, or civil

---

(footnote continued from preceding page)
18 U.S.C. § 2510(15). A "provider of e-mail services [is] undisputedly an ECS. *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 902 (9th Cir. 2008) *rev'd on other grounds sub nom. City of Ontario v. Quon*, 130 S. Ct. 2619 (2010). By providing users the ability to send and receive emails and instant chats with other users, TradeKey is an ECS under the SCA. *See* SACC ¶ 5, 22-23.

[3] A provider can also disclose content in order to deliver the communication to its destinations, or to protect itself. *See* 18 U.S.C. § 2702(b)(1), (4)-(5).

litigants generally. Congress' detailed listing of exceptions for disclosure creates a presumption that that "all omissions should be understood as exclusions." *Silvers v. Sony Pictures Entertainment, Inc.*, 402 F.3d 881, 885 (9th Cir. 2005) (internal quotations and citation omitted). The specific omission of Lanham Act seizures and civil litigation from the SCA exceptions in 18 U.S.C. §§ 2701 and 2702 means Congress did not believe access to stored electronic content was appropriate for these disputes.

2. The Lanham Act In General, and the May 2011 Seizure Order Specifically, Do Not "Authorize" Access to the Contents of Electronic Communications Under the SCA.

Counterclaim defendants assert the signed seizure order meant they had "authorization" to seize the contents of communication under 18 U.S.C. § 2701(a) because the Lanham Act trumps the SCA and authorizes the civil seizure of stored electronic communications. The "short answer is that Congress did not write the statute that way." *United States v. Naftalin*, 441 U.S. 768, 773 (1979). The Lanham Act does not "authorize" access to the contents of electronic communications. Moreover, to the extent the May 2011 seizure order permitted the seizure of the content of stored electronic communications, it was invalid and thus failed to "authorize" any seizure.

a. The Lanham Act Does Not "Authorize" Access to the Content of Stored Electronic Communications.

The seizure provision of the Lanham Act permits a court to order the seizure of items potentially involved in trademark infringement:

> the court may, upon *ex parte* application, grant an order . . . providing for the seizure of goods and counterfeit marks involved in such violation and the means of making such marks, and records documenting the manufacture, sale, or receipt of things involved in such violation.

15 U.S.C. § 1116(d)(1)(A). Seizure is an "extraordinary mechanism," particularly because it is *ex parte*. *In re Lorillard Tobacco Co.*, 370 F.3d 982, 989 (9th Cir. 2004); *see also Major League Baseball Promotion Corp. v. Colour-Tex, Inc.*, 729 F. Supp. 1035, 1047 (D.N.J. 1990) (noting "extraordinary nature of the *ex parte* seizure remedy" in 15 U.S.C. § 1116(d)). Congress recognized Lanham Act seizures were reserved for "extreme circumstances" and required courts "to use extreme caution before issuing a seizure order." *Skierkewiecz v. Gonzalez*, 711 F. Supp. 931, 934 (N.D. Ill. 1989).

Notably, nothing in 15 U.S.C. § 1116(d) refers to the contents of electronic communications. The seizure provision of the Lanham Act was enacted in 1984, before the SCA's enactment in 1986. *See* S. Rep. No. 98-526 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3627. Email and electronic communication was an emerging

technology, but still not widely available to the public in 1984. In fact computers themselves were not nearly as ubiquitous as they are today. According to the census bureau, in 1984, only 8% of households in the United States had a computer at home. By 2003, that percentage had jumped to 62%. And by 2009, 69% of households reported using the Internet at home.[4] In 1984, there was no World Wide Web, Yahoo! or Gmail, let alone the forms of communication that have exploded in popularity now, like Facebook, Twitter, and LinkedIn.

Given the realities of 1984, Congress was clearly focused on giving private parties the ability "to seize counterfeit goods" themselves before they could be destroyed. S. Rep. 98-526, 2-3, 1984 U.S.C.C.A.N. at 3628-29; *see also Waco Int'l, Inc. v. KHK Scaffolding Houston Inc.*, 278 F.3d 523, 532 (5th Cir. 2002) ("the primary focus of an *ex parte* seizure order is on the goods themselves"). As a result, nothing in 15 U.S.C. § 1116(d)(1)(A) specifically allows for the seizure of content stored by an electronic communications provider.

When Congress enacted the SCA two years later, it made absolutely no mention of the Lanham Act. While the SCA carved out guidelines for law enforcement to access the contents of electronic communications from providers, it was noticeably silent with respect to civil litigation. "Congress is, of course,

[4] *See* United States Census Bureau Publications About Computer and Internet Use, Appendix Table A: Households With a Computer and Internet Use: 1984 to 2009, available at https://www.census.gov/hhes/computer/publications/, last accessed October 24, 2012.

presumed to know existing law pertinent to any new legislation it enacts." *United States v. LeCoe*, 936 F.2d 398, 403 (9th Cir. 1991) (citing *Native Village of Venetie v. Alaska*, 918 F.2d 797, 803 (9th Cir. 1990)). So when Congress decides not to speak, its silence controls. *See BFP v. Resolution Trust Corp.*, 511 U.S. 531, 537 (1994) ("it is generally presumed that Congress acts intentionally and purposely when it includes particular language in one section of a statute but omits it in another") (internal quotations, citation and brackets omitted). Here, that silence means the Lanham Act was not a mechanism through which civil litigants could access the content of stored electronic communications from communication providers. This was consistent with the SCA's purpose of protecting electronic information from disclosure by "unauthorized private parties." S. Rep. No. 99-541, at 3, 1986 U.S.C.C.A.N. at 3557.

Since the Lanham Act neither authorizes the disclosure of the contents of electronic communications itself, nor is found within the exceptions to the SCA, it cannot authorize a communications provider to disclose content. *See e.g., Boudette v. Barnette*, 923 F.2d 754, 757 (9th Cir. 1991) ("if a statute states that a party can invoke an action by request, such request is presumed the exclusive manner in which the action may be invoked.). As noted above, "all omissions should be understood as exclusions." *Silvers*, 402 F.3d at 885. That is precisely how other courts interpreting the SCA have determined that private litigants in civil lawsuits cannot compel disclosure of content from a communications provider. *See Bower v. Bower*, 808 F.

Supp. 2d 348, 350 (D. Mass. 2011) ("pursuant to § 2703, governmental entities may require the disclosure of the contents of customers' electronic communications or subscriber information in the context of ongoing criminal investigations, but no similar authority is granted to civil litigants"); *In re Subpoena Duces Tecum to AOL*, 550 F. Supp. 2d at 609 ("the plain language of the [SCA] prohibits AOL from producing the [] emails, and the issuance of a civil discovery subpoena is not an exception to the provisions of the [SCA]"); *O'Grady v. Superior Court*, 139 Cal. App. 4th 1423, 1447, 44 Cal. Rptr. 3d 72, 89 (2006) (because the SCA "makes no exception for civil discovery" it "must be applied, in accordance with its plain terms, to render unenforceable the subpoenas seeking to compel [communication providers] to disclose the contents of emails stored on their facilities.").

In short, neither the Lanham Act nor the SCA authorize a communications provider to disclose the contents of electronic communications in civil litigation.

b. The Seizure Order In This Case Was Not Valid "Authorization."

Even if this Court were to find the Lanham Act somehow "authorizes" the seizure of the content of stored electronic communications, the May 2011 seizure order cannot qualify as legally valid "authorization," since it calls for a violation of the SCA. A judicial order that purports to permit a seizure otherwise not permitted under the law is invalid and leads to, in effect, an *unauthorized* seizure.

The Supreme Court has reached this conclusion in the context of deficient search warrants. In *Groh v. Ramirez*, 540 U.S. 551 (2004), the Court found a search

warrant signed by a magistrate judge that failed to describe the items to be searched – in violation of the Fourth Amendment's particularity requirement – "so obviously deficient" that the search had to be regarded as warrantless, or unauthorized. 540 U.S. at 558. Most critically, the court denied qualified immunity to the officers, finding the search to be unreasonable despite the presence of a signed search warrant because "[n]o reasonable officer could claim to be unaware of the basic rule, well established by our cases, that, absent consent or exigency, a warrantless search of the home is presumptively unconstitutional." *Id.* at 564 (citing *Payton v. New York*, 445 U.S. 573, 586-588 (1980)).

When it comes to the SCA, the Ninth Circuit dealt with a situation similar to the one here in *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2003), where it found an invalid subpoena could not "authorize" access to stored communications under the SCA. 359 F.3d at 1073-75. There, a law firm issued a subpoena to an email provider, seeking copies of all emails in relation to a commercial litigation dispute. *Id.* at 1071. After the magistrate found the subpoena "massively overbroad" and "patently unlawful," the email holders sued the law firm alleging, among other things, SCA violations. *Id.* at 1071-72. The district court found no SCA violation because the communications provider had "authorized" the access on the basis of the subpoena it complied with. *Id.* at 1072. The Ninth Circuit reversed, finding that the improper subpoena could not provide "authorization" under the SCA because its

"falsity transformed the access from a bona fide state-sanctioned inspection into private snooping." *Id.* at 1073.

Regardless of whether there was "falsity" or bad faith here, the fact remains that a seizure order that violates the SCA does not provide the type of "authorization" needed to access stored communications under 18 U.S.C. § 2701. Like *Groh*, the failure of the seizure order to restrict access to the content of stored electronic communications rendered the order effectively null and void, making the seizure unauthorized. Therefore any reliance on the clearly deficient seizure order is unreasonable. The order failed to "authorize" any disclosure under the SCA.

Moreover, allowing the seizure order here to somehow condone an otherwise illegal act sets a dangerous precedent for civil litigants everywhere. Subpoenas are issued with no judicial supervision at all, and it is easy to imagine creative ways in which litigants can attempt to obtain content from electronic communication providers in highly charged emotional disputes, like a custody battle. *See* Fed. R. Civ. P. 45(a)(3); *Theofel*, 359 F.3d at 1074 ("[t]he subpoena power is a substantial delegation of authority to private parties"). With the growing popularity of social media sites like Facebook, Twitter and LinkedIn that have their own built-in email and instant messaging systems, the amount of data that can be seized becomes endless. Litigants can make broad requests for data through seizure orders, subpoenas and other legal process, obtaining enormous amounts of sensitive data about who a person communicates with, when they communicate, and about what. It

will be up to the individual communication providers to challenge the orders, and many will be uninterested in the fight. To claim that a judicial seal of approval somehow "authorizes" otherwise invalid access to stored electronic content would wreak havoc and clearly violate the stricture of the SCA. This Court should not sanction this type of fast and loose behavior.

c. Lanham Act Litigants Should Not Be "Authorized" to Seize the Contents of Electronic Communications More Broadly Than Law Enforcement.

While counterclaim defendants argue that applying the plain text of the SCA "would severely undermine seizures under the Lanham Act, given that most evidence today is electronic," this Court should resist the urge to create a broad exception to the SCA that undermines its very purpose. *See* Motion to Dismiss Counterclaims, Doc. 394, p. 15.

There is no doubt the SCA's strong privacy protection creates inconvenient situations for litigators who cannot access content the same way law enforcement can. One pair of commentators, for example, have lamented the SCA's failure to allow criminal defendants access to potentially exculpatory contents of electronic communications. *See* Marc J. Zwillinger, Christian S. Genetski, *Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not A Level Playing Field*, 97 J. Crim. L. & Criminology 569, 584 (2007) (SCA has "no general exception for disclosures made pursuant to legal process or where otherwise required

by law."). But just as criminal defendants have had to adapt to the strictures of the SCA, so too must civil litigants.

Interpreting the SCA in the way requested by counterclaim defendants would defeat the SCA's privacy protections altogether and give civil litigants easier access to a provider's inventory of the contents of electronic communications than law enforcement. After all, over 9 million emails and 71,000 stored chats were accessed here. SACC ¶¶ 48, 66. Undoubtedly most of this content has nothing to do with the trademark infringement dispute whatsoever. In arguing there is no claim for an SCA violation in this case, counterclaim defendants imply that a civil litigant has a right to seize wholesale the contents of electronic communications from a provider without making any effort to segregate data relevant to the legal dispute from data that is irrelevant. Not even law enforcement – who *is* authorized to access the contents of communication under the SCA – has this broad power.

First the SCA requires the government to obtain a search warrant for messages in electronic storage for less than 180 days. 18 U.S.C. § 2703(a). In the Ninth Circuit, that includes opened emails stored with a communications provider for less than 180 days. *See Theofel*, 359 F.3d at 1076-77.[5] Even for older emails, the SCA

[5] The Sixth Circuit requires a search warrant to obtain the contents of all email notwithstanding the 180-day marker in the SCA. *See United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) ("to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional.").

still requires law enforcement to obtain a search warrant if it does not want to notify the customer ahead of time. 18 U.S.C. § 2703(b)(1)(A).[6]

Of course a search warrant requires law enforcement to demonstrate probable cause, or a "a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). Probable cause is required because "no intrusion at all is justified without a careful prior determination of *necessity*." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971) (emphasis added). Additionally, search warrants must be "as limited as possible" to avoid "a general, exploratory rummaging in a person's belongings." *Id.* When it comes to seizing electronic data, the Ninth Circuit has called for "greater vigilance on the part of judicial officers" to ensure the "process of segregating electronic data that is seizable from that which is not [does] not become a vehicle for the government to gain access to data which it has no probable cause to collect." *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc) (per curiam).

As a result of these limitations, law enforcement is unable to obtain the broad seizure order that issued here. For example, one court recently denied a request for a

[6] Only if law enforcement notifies the customer can it obtain content without a search warrant. 18 U.S.C. § 2703(b)(1). But even then, law enforcement must still obtain an administrative or grand jury subpoena, or a judicial order after demonstrating "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication . . . are relevant and material to an ongoing criminal investigation." 18 U.S.C. §§ 2703(b)(1)(B), 2703(d).

search warrant seeking access to the "contents of all e-mails" associated with an email account suspected of sending fraudulent spam. *In re Applications for Search Warrants for Info. Associated with Target Email Address*, 12-MJ-8119-DJW, 2012 WL 4383917, *1 (D. Kan. Sept. 21, 2012). The court found the warrant "too broad and too general," noting it failed "to limit the universe of electronic communications and information to be turned over" by the email provider, and failed "to set out any limits on the government's review of the potentially large amount of electronic communications and information obtained from the electronic communications service providers." *Id.* at *8.

The broad seizure counterclaim defendants assert is authorized by the Lanham Act, however, has nothing approaching these limiting principles. The person requesting a seizure must only demonstrate that she is "likely to succeed." 15 U.S.C. § 1116(d)(4)(B)(iii). While the order itself must have "a particular description of the matter to be seized, and a description of each place at which such matter is to be seized," it has no built-in limitations for *what* is to be seized. 15 U.S.C. § 1116(d)(5)(B). In theory such seizures should be limited to the "seizure of goods and counterfeit marks" and "the means of making such marks, and records documenting the manufacture, sale, or receipt of things involved in such violation." 15 U.S.C. § 1116(d)(1)(A). But the broad seizure in this case highlights the Lanham Act's inadequacy in truly narrowing what can and cannot be seized. When the item to be seized is a website and the equipment hosting it purporting to contain "records

documenting the manufacture, sale, or receipt" of counterfeit goods, it is inevitable that irrelevant records will be swept up as well. And that is precisely what happened here: counterclaim defendants were able to obtain 9 million stored emails and 71,000 stored chats, including contents of communications that have no connection to the trademark infringement dispute and should not have been seized. SACC ¶¶ 48, 66.

Such a haul would make law enforcement envious. Private litigants should not be given broader access to the content of electronic communications if law enforcement – the only entity with explicit statutory authorization under the SCA to seize this content – is itself limited in accessing this data.

B. The Lanham Act Can Be Interpreted Consistently With the SCA To Give Civil Litigants A Seizure Remedy Without Intruding on Electronic Privacy.

Counterclaim defendants argue that the Lanham Act and SCA conflict with each other, and that ultimately the "Lanham Act's specific statutory framework for seizures of counterfeit goods cannot be supplanted or rendered void by a subsequent, more general statute, such as the SCA." Motion to Dismiss Counterclaims, Doc. No. 394, page 7. But this ignores the fact that the SCA and Lanham Act can coexist.

When a court "can construe two statutes so that they conflict, or so that they can be reconciled and both can be applied, it is obliged to reconcile them." *Momeni v. Chertoff*, 521 F.3d 1094, 1097 (9th Cir. 2008) (citing *Cal. ex rel. Sacramento Metro. Air Quality Mgmt. Dist. v. United States*, 215 F.3d 1005, 1012 (9th Cir. 2000)

("Of course, it is a well established axiom of statutory construction that, whenever possible, a court should interpret two seemingly inconsistent statutes to avoid a potential conflict.")). Any imagined conflict between the Lanham Act and the SCA can easily be reconciled: a Lanham Act seizure order can authorize a communications provider to disclose "records documenting the manufacture, sale, or receipt of things" involved in a trademark infringement dispute, provided that no contents of electronic communications are seized. 15 U.S.C. § 1116(d)(1)(A).[7] Both the SCA and the Lanham Act specifically envision this.

The SCA permits a communications provider to disclose non-content records, including "a record or other information pertaining to a subscriber to or customer of such service" to "any person other than a government entity." 18 U.S.C. § 2702(c)(6); *see also* Kerr, *A User's Guide to the Stored Communications Act*, 72 Geo. Wash. L. Rev. at 1222 ("noncontent records can be disclosed to nongovernment entities without restriction"). Indeed, the SCA expressly lists noncontent information that can be obtained by law enforcement without a search warrant, including:

(A) name;

[7] And even if there is a conflict, the SCA is the specific statute that controls here. "[I]t is a commonplace of statutory construction that the specific governs the general." *Morales v. Trans World Airlines, Inc.*, 504 U.S. 374, 384 (1992). While the Lanham Act broadly permits the seizure of "records documenting the manufacture, sale, or receipt" of potentially infringing goods, the SCA specifically prohibits the seizure of stored electronic communications from communications providers save for a few enumerated exceptions. *See* 15 U.S.C. § 1116(d)(1)(A), 18 U.S.C. §§ 2701(a), (c), 2702(b).

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number).

18 U.S.C. § 2703(c)(2). It follows that a Lanham Act seizure can authorize a communications provider to release similar information under 15 U.S.C. § 1116(d) without running afoul of the SCA's rigid prohibition against the disclosure of content.

Similarly, the Lanham Act provides a court with some tools to ensure a seizure does not intrude completely on the rights of others. The court can issue an order "to protect the defendant from undue damage from the disclosure" of "confidential information during the course of the seizure," including an order "restricting the access of the applicant" to the confidential information. 15 U.S.C.A. § 1116(d)(9). A court ordering a Lanham Act seizure must require the seizing party to comply with the SCA by restricting access to the contents of "confidential information," specifically the contents of electronic communications.

This Court is obligated to reconcile the SCA and Lanham Act. The only way to do that is to find that a Lanham Act seizure does not authorize access to the content of stored electronic communications held by a communications provider.

CONCLUSION

Congress omitted civil litigants from the exceptions to the SCA for a good reason: to ensure the content of electronic communications were not spilled out in the open for the public to see in the course of civil litigation. Nothing in the Lanham Act warrants second guessing Congress' decision. The broad seizure here allowed counterclaim defendants to seize more than what law enforcement, the *only* entity authorized under the SCA to obtain the contents of electronic communications from a provider, can similarly obtain. Because Congress did not intend such an absurd result – a result that would lead to significant privacy concerns – this Court should deny the motion to dismiss the counterclaims.

Dated: October 25, 2012

Respectfully submitted,

/s/ *Hanni M. Fakhoury*
Hanni M. Fakhoury
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x108
Facsimile: (415) 436-9993

Attorneys for Amicus Curiae
ELECTRONIC FRONTIER FOUNDATION