IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

ASIS INTERNET SERVICES, et al.

Plaintiffs,

v.

ACTIVE RESPONSE GROUP et al.,

Defendants.

NO. C07 6211 TEH

ORDER RE: DESIGNATION OF EMAIL ADDRESSES UNDER PROTECTIVE ORDER; ORDER APPOINTING SPECIAL MASTER

The Court reviewed the Parties' briefs, filed April 21, 2008 and May 5, 2008, in support of and in opposition to Plaintiff's request for a Protective Order designating the email addresses to which the emails at issue in this case were sent "Highly Confidential – Attorney's Eyes Only," and heard argument on this matter on Monday, May 19, 2008. For the reasons set out below, the email addresses shall be designated "Confidential" pursuant to a modified protective order, as set out below.

**BACKGROUND**

Plaintiffs are Internet Access Providers ("IAPs") who provide internet service to individual customers. Defendant ARG Active Response Group is an internet marketer that hires subcontractors to send bulk commercial emails and thereby generate visitors for its customers' websites. The Complaint alleges that Defendants and related entities (collectively "ARG") sent thousands of unsolicited and misleading spam email messages to Plaintiffs' customers, in violation of the Controlling the Assault of Non-Solicited Pornography and Marketing ("CAN-SPAM") Act of 2003, 15 U.S.C. § 7704, and California Bus. & Prof. Code § 17529.5 (unlawful activities relating to commercial email advertisements).

ARG denies that it sent commercial emails to anyone, and claims that only its third-party contractors do so. ARG sought discovery of all the spam emails at issue to determine who sent the email "by having an employee examine the email addresses to which emails were allegedly sent." ARG Reply Brief, filed May 5, 2008 ("ARG Reply") at 2. Plaintiffs agreed to disclose the emails, and the parties agreed that the disclosures should generally be subject to the Court's standard protective order. The only dispute is whether the "sent to" field of the emails – the portion which lists the email addresses of Plaintiffs' current or former clients, or Plaintiffs' administrative email addresses – should be designated "Confidential" or "Highly Confidential – Attorney Eyes Only."

Plaintiffs seek an order designating the email addresses "Highly Confidential – Attorneys' Eyes Only," and made available only to Defendants' attorneys and experts. ARG argues that the email addresses should be designated "Confidential," with the exception that Defendant may disclose the email addresses "as is reasonably necessary to determine the identity of the emails' senders" to its Affiliates and contractors or subcontractors. .

Under § 2.3 of this Court's standard protective order, a "Confidential" designation is for "information (regardless of how generated, stored, or maintained) or tangible things that qualify for protection under standards developed under Fed. R. Civ. Pro. 26(c)." Fed. R. Civ. Pro. 26, in turn, provides that the Court may, for good cause, issue a protective order to protect a person or party from various undue burdens, including: "requiring that a trade secret or other confidential research, development or commercial information not be revealed or be revealed only in a specified way." Fed. R. Civ. Pro. 26(c)(1)(G). The language of the Court's standard protective order provides that "Confidential" information may only be divulged to the court and to party's outside counsel, employees, experts and court reporters to whom disclosure is "reasonably necessary" for the litigation and who must sign an agreement to be bound by the Protective Order. Prot. Order § 7.2(b).

The Protective Order defines "Highly Confidential– Attorneys' Eyes Only" information or items, on the other hand, as "extremely sensitive 'Confidential Information or Items' whose disclosure to another Party or non-party would create a substantial risk fo

serious injury that could not be avoided by less restrictive means." *Id.* § 2.4. Such information can only be disclosed to the court and to party's outside counsel, in house counsel, experts, and court reporters who have signed an agreement to be bound by the Protective Order. *Id.* § 7.3.

**DISCUSSION**

**I. Whether Disclosure Is Barred By Law**

Plaintiffs argue that the email addresses should receive the highest level of protection because Plaintiffs are prohibited from disclosing them under two federal statutes and the California constitutional right to privacy. None of these bars disclosure.

**A. Children's Online Privacy Protection Act**

Plaintiffs allege that the Children's Online Privacy Protection Act, 15 U.S.C. § 6501-6506 ("COPPA") requires them to protect from disclosure any information relating to or that can be used to identify a child (anyone under 13). Plaintiffs argue that since they sell their email accounts to families, their customers likely include children, and forcing them to disclose address lists would cause them to violate COPPA.

COPPA does not bar disclosure here. The statute provides that violation of its implementing regulations is unlawful. 15 U.S.C. § 6502. The regulations provide that internet providers must, among other things, "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children," 16 C.F.R. §§ 312.3(e), 312.8, and to seek parental consent for "collection, use, or dissemination" of personal information from a child, 16 C.F.R. §§ 312.3(b), 312.5.

Plaintiffs IAPs do not appear to be covered by COPPA. Although the regulations themselves define an "operator" as "any person who operates ... an online service" for commercial purposes "and who collects or maintains personal information from or about the users of or visitors to such website or online service," 16 C.F.R. § 312.2, the Federal Trade Commission interprets this regulation as providing that "entities that merely provide access to the Internet, without providing content or collecting information from children" are not

considered "operators" and are therefore not covered by the Act or Regulations. Children's Online Privacy Protection Rule, 64 Fed.Reg. 59888, 59891 (November 3, 1999) and 64 Fed.Reg. 22750, 22752 (April 27, 1999) (notice of proposed rulemaking). Moreover, the COPPA regulations apply to "any operator that has *actual knowledge* that it is collecting or maintaining personal information from a child," 16 C.F.R. § 312.3 (emphasis added); while Plaintiffs argue that their accounts are "let to families," they do not allege they have "actual knowledge" that they are collecting information about children. AsIs Opening Brief, filed April 21, 2008 ("AsIs Brief") at 2. Finally, although neither party cites to this section, the statute makes an exception to the parental consent requirement if such information is necessary to "(i) to protect the security or integrity of [the service provider's] website; (ii) to take precautions against liability; (iii) to respond to judicial process." § 6502(b)(1)(E); 16 C.F.R. § 312.5(c)(5) (same); 64 Fed. Reg. at 59902 and n.225 ("the operator may collect, use, or disseminate such information as necessary to protect the security or the integrity of the site or service, to take precautions against liability, [or] to respond to judicial process" and "an operator may collect limited information in order to protect the security of its site, for example, from hackers"). Thus, even if Plaintiffs are covered by COPPA, disclosing the email addresses during discovery in order to allow ARG to determine who sent the spam emails falls into the first and third exceptions to the parental consent rule.

**B. Telecommunications Act of 1996**

Plaintiffs next argue that common carriers providing wire communications access must "protect aggregate information including customer proprietary information" under the privacy provisions of the Telecommunications Act of 1996, 47 U.S.C. § 222. That statute provides that

> Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier.

*Id.*

ARG argues that Plaintiffs are not "telecommunications carriers" within the meaning of the Act. A "telecommunications carrier" is a provider of "telecommunications services" as defined in the Communications Act of 1934. 47 U.S.C. §§ 153(44) and (46); 47 C.F.R. § 64.2003(o), (p) (adopting definitions in Communications Act of 1934). Broadband internet access service is an "information service," not a "telecommunications service" under that statute. *See Time Warner Telecom, Inc. v. Federal Communications Commission*, 507 F.3d 205 (3d Cir. 2007) (upholding FCC's construction of the statute in "Appropriate Framework for Broadband Access to the Internet over Wireline Facilities," 20 F.C.C. Rcd. 14853 (2005)); *National Cable & Telecommunications Ass'n v. Brand X Internet Services*, __ U.S. __, 125 S.Ct. 2688 (2005) (upholding FCC's construction of statute in "In the Matter of Federal-State Joint Board on Universal Service, 13 F.C.C. Rcd. 11501, 11536-40 (1998)).

Even if Plaintiffs are telecommunications carriers, the email addresses alone do not fall within the definition of "consumer proprietary network information," which receives the highest level of protection under the Act. *See* 47 U.S.C. § 222(h)(1)(A)(CPNI is "information that related to the quantity, technical configuration, type, destination, location and amount of use of a telecommunication service subscribed to by any customer"); *U.S. West, Inc. v. F.C.C.*, 182 F.2d 1224, 1229 n.1 (10th Cir. 1999)(§ 222 protects three types of customer information: CPNI, aggregate customer information, and subscriber list information; of those, CPNI receives the "highest level of privacy protection," and other types are afforded "substantially less privacy protection"). Plaintiffs argue that the email lists "likely" fall within the definition of "aggregate information" that they are required to protect, so at best the information would require less protection than the "attorney's eyes only" protection requested. *See ICG Communications, Inc. v. Allegiance Telecom*, 211 F.R.D. 610 (N.D. Cal. 2001)(ordering disclosure of CPNI, subject to "attorney eyes only" protective order, because court-ordered discovery response falls within exception under § 222(c)(1) for disclosures "required by law").

Finally, § 222 allows carriers to "us[e], disclos[e], or permit[] access to customer proprietary network information obtained from its customers, either directly or indirectly

through its agents ... to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." § 222(d)(2). As above, the disclosures fall within this exception.

**C. Right to Privacy**

Although the right to privacy does protect certain email addresses at issue, it does not entirely bar disclosure.

Plaintiffs argue that disclosure would violate their customers' right to privacy under the California Constitution Article I, Section 1, which protects against "dissemination or misuse of sensitive and confidential information." *Hill v. National Collegiate Athletic Assn.*, 7 Cal.4th 1, 35 (1994). Although privileges are determined under federal law in this federal question case, Fed. R. Evid. 501; *United States v. Zolin*, 491 U.S. 554, 562 (1989), the Court should take into account state privileges as a matter of comity where it can do so "at no substantial costs to federal substantive and procedural policy." *Leon v. County of San Diego*, 202 F.R.D. 631, 635 (S.D.Cal. 2001). The California right to privacy "is not an absolute right, but a right subject to invasion depending upon the circumstances. Moreover, courts have frequently found that a party's need for the information may outweigh whatever privacy rights, if any, another party may have. *Oakes v. Halvorsen Marine Ltd.*,179 F.R.D. 281, 284 (C.D.Cal. 1998)(citations omitted).

The privacy interest here is negligible. While Plaintiffs' customers (and former customers) have some privacy interest in their email addresses, *see, e.g., Center For Public Integrity v. F.C.C.* 505 F.Supp.2d 106, 113 (D.D.C. 2007)(allowing agency to withhold employee email addresses because disclosure would constitute invasion of privacy), Plaintiffs' Complaint states that the email addresses at issue are all inactive or administrative, Complaint ¶¶ 17, 25, 36. Magistrate Judge LaPorte has held that "there is no consumer privacy or commercial value to protect" in a list of email accounts that are inactive or have never been active. *Phillips v. Netblue, Inc.*, 2006 WL 3545002 (N.D. Cal. December 8, 2006). At the hearing, Plaintiffs clarified that some unknown number of the Foggy.net email addresses are those of consumers.

Although Plaintiffs argue that "publicly disclosing thousands of email addresses to hundreds or thousands of internet marketers" could lead to the misuse of normally confidential information,[1] Plaintiffs have not shown that disclosure will inevitably lead to harm even if a protective order is in place. Notably, Plaintiffs' counsel failed to answer direct questions posed by the Court at the hearing about what harm might ensue if the email addresses are disclosed subject to a protective order, and whether a protective order would provide adequate protection. California courts have held that if intrusion into privacy is limited and "confidential information is carefully shielded from disclosure except to those who have a legitimate need to know, privacy concerns are assuaged." *Hill*, 7 Cal.4th at 38.

## II. The Email Addresses Will Be Designated "Confidential" and Subject To Disclosure Under A Modified Protective Order

To be entitled to a "Highly Confidential – Attorney's Eyes Only" designation, Plaintiffs must show that the email addresses are material "whose disclosure to another Party or non-party would create a substantial risk of serious injury that could not be avoided by less restrictive means."

ARG is seeking disclosure of the emails to at least a substantial number of third parties. It asserts that it needs the lists to determine who actually sent the spam emails.[2] ARG's Chief Technology officer explained that to do so, ARG would check to see if its affiliates and their vendors have the email addresses on their permission or suppression lists. Brown Decl. ¶ 8. Because Defendant's counsel declined at the hearing to address the

[1] Plaintiffs allege the list could be sold, or that Plaintiffs could be vulnerable to "denial of service attacks" (the servers could be flooded with emails until they can no longer operate) or a "directory harvest" of the emails.

[2] Plaintiffs argue, without evidentiary support, that Defendants can use "link tracking" software to tell how the users got to their webpage, but ARG's Chief Technology Officer Brady Brown declares that ARG cannot identify who sent the emails by examining the links in the emails. Declaration of Brady Brown in Support of Brief filed by Active Response Group, Inc., filed May 5, 2008 ("Brown Decl.") ¶¶ 5-6.

Court's questions about the mechanics of the process,[3] the Court will assume Plaintiffs correctly contend that this would involve disclosing the email address list to "hundreds or thousands" of bulk emailing contractors.

Nonetheless, as set out above, Plaintiffs have not explained why requiring those third parties to sign the agreement to be bound by the protective order is insufficient protection. The standard Protective Order provides that any information disclosed may be used "only for prosecuting, defending, or attempting to settle this litigation," Prot. Order § 7.1, and the Agreement to be Bound provides that violating the Protective Order will expose the violator to "sanctions and punishment in the nature of contempt." *Id.* Exh. A.

Plaintiffs suggested that the sheer number of third parties to whom the list is disclosed could be reduced if ARG is permitted to disclose the email addresses for comparison purposes only to its affiliates, vendors, or other third parties whose own permission, suppression, or other comparison lists contain names with "Foggy" or "AsIs" domain names. At the hearing on this matter, Defendant offered no substantive opposition to using this winnowing process. Accordingly, the permission to disclose the email addresses to third parties for the purpose of identifying the sender set out in section 7.4 of the Court's Protective Order in this case applies only to those third parties who have stated that they have a "Foggy" or "AsIs" domain name on the list of email addresses to be used for comparison.

Finally, the Court will require any entity or individual to whom the email addresses are disclosed to sign the "Agreement to be Bound by Protective Order," will require Defendant to retain all the signed Agreements, and to convey the names of those third parties to Plaintiffs prior to actual disclosure. Other than arguing that these requirements improperly

[3] The Court asked how Defendant plans to use the email addresses to determine who sent the emails, whether ARG plans to provide the list to its "affiliates" and/or their vendors to see if the emails are on their permission or suppression lists, as suggested in paragraph 8 of Mr. Brown's declaration, what proportion of the addresses does it plans to disclose, and to how many entities, and whether there were any objective measures that the Defendant, Plaintiffs, or Court could use to determine whether ARG's affiliates and/or their vendors to whom ARG intends to disclose the addresses employ verifiable privacy practices or, alternately, have engaged in spamming abuses. The Court warned that parties were not required to answer the questions, but the Court would assume the answers were unfavorable if a party failed to do so.

"assume" that ARG, its vendors, affiliates, or their subcontractors will engage in spamming abuses, Defendants have offered no concrete reasons why the Court should not impose these additional protections. Accordingly, these additional protections are set out in Section 7.4 of the Court's Protective Order filed herewith.

Discovery in this case may involve further complex technical issues, and the parties have not shown a willingness or ability to solve such problems cooperatively. The Court, including its Magistrate Judges, should not be burdened with further disputes relating to disclosure or designation under the Protective Order or other related discovery disputes. As another judge in this district explained long ago:

> The discovery system depends absolutely on good faith and common sense from counsel. The courts, sorely pressed by demands to try cases promptly and to rule thoughtfully on potentially case dispositive motions, simply do not have the resources to police closely the operation of the discovery process. The whole system of Civil adjudication would be ground to a virtual halt if the courts were forced to intervene in even a modest percentage of discovery transactions. That fact should impose on counsel an acute sense of responsibility about how they handle discovery matters. They should strive to be cooperative, practical and sensible, and should turn to the courts (or take positions that force others to turn to the courts) only in extraordinary situations that implicate truly significant interests.

*In re Convergent Tech. Sec. Litig.*, 108 F.R.D. 328, 331 (N.D. Cal. 1985). A discovery master is necessary to avoid wasting judicial resources and preventing a timely resolution of this case.

Accordingly, with good cause appearing, IT IS HEREBY ORDERED that:

1. Edward Swanson, Esq., of Swanson, McNamara, & Haller, LLP, is appointed as Special Master to supervise and preside over all remaining discovery in this case.

a. If necessary, the Special Master may attend all or portions of depositions, rule on all objections made by counsel during the depositions, rule on any instructions by counsel for the deponent not to answer a question, and order the deponent to respond to questions.

b. The Special Master shall immediately notify this Court if, during a deposition in which he is in attendance, any counsel fails to comply or cooperate fully with any of the Special Master's rulings.

2. The Special Master shall have discretion to hear discovery matters on shortened time, and shall also have authority to recommend to the Court new discovery deadlines and/or to recommend that case management conferences be rescheduled, as appropriate.

3. Federal Rule of Civil Procedure 53 shall apply to proceedings before the Special Master, except that the parties shall have 10 days to Object or Move to Adopt or Modify an order, report, or recommendation by the Special Master, rather than the 20 days set out in Rule 53(f)(2).

4. The Special Master's hourly fee shall be $450.00. The presumption shall be that the Special Master's fees will be split evenly between the parties; the Special Master shall, however, have discretion to allocate and assess the payment of his fees among the parties as he believes appropriate, for each issue that arises. The parties shall pay the Special Master's fees within ten calendar days of assessment, unless otherwise excused by the Special Master or this Court.

5. At his earliest convenience, the Special Master shall contact the parties to discuss the execution of his duties in connection with this Order, including procedures under § 6.3 of the Protective Order.

**IT IS SO ORDERED.**

Dated: May 20, 2008

THELTON E. HENDERSON, JUDGE
UNITED STATES DISTRICT COURT