IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OPTINREALBIG.COM, LLC,

Plaintiff,

v.

IRONPORT SYSTEMS, INC. and its wholly owned subsidiary, SPAMCOP.NET, INC.,

Defendants.
_____/

No. C 04-1687 SBA

ORDER DENYING PLAINTIFF'S MOTION FOR PRELIMINARY INJUNCTION

[Docket Nos. 24, 53]

This matter comes before the Court on the motion for a preliminary injunction filed by plaintiff OPTINREALBIG.COM, LLC ("OptIn") to enjoin certain activities of defendant SPAMCOP.NET, Inc. ("SpamCop") a wholly owned subsidiary of IronPort Systems, Inc. Having read and considered the arguments presented by the parties in their moving papers, and at the May 18, 2004 hearing, the Court hereby DENIES OptIn's motion for preliminary injunction.

I. ADMINISTRATIVE ISSUES

During the May 18, 2004 hearing, the Court specifically requested a supplemental declaration from SpamCop that explained technical issues regarding how SpamCop's software functions. The Court did not request the same from OptIn. Nevertheless, OptIn took the liberty of submitting not only supplemental declarations to bolster its arguments, but a supplemental brief regarding issues related to the Communications Decency Act. Notably, OptIn's submissions were filed on May 25, 2004, a week after the Court held oral argument. Such uninvited submissions are inappropriate and violate the notions of fairness that underlie the judicial process. OptIn should be aware that future abuses of the judicial process may result in sanctions.

The Court GRANTS SpamCop's motion to strike the supplemental brief and declarations. [Docket No. 53]. Lest there be any doubt, even if the Court had considered the supplemental filings, they

would not change the Court's determination regarding OptIn's motion for a preliminary injunction or the Court's reading of the Communications Decency Act. The supplemental declarations and briefing are not persuasive and, in fact, at some points actually bolster SpamCop's position.

II. BACKGROUND

At the center of this case is a debate about bulk commercial e-mails, whether they are legitimately solicited or unsolicited mail known as SPAM, about those who make a living sending bulk commercial e-mails, about those who make a living trying to destroy spam senders, and about how these two business can coexist. Plaintiff in this case, OptIn, is in the business of sending bulk commercial e-mails. Defendant, SpamCop, is in the business of collecting complaints from recipients of alleged spam and forwarding these complaints to Internet Service Providers ("ISPs") who supply internet bandwidth to the purported spammers. OptIn alleges that SpamCop has inflated the complaints against OptIn, which has in turn caused ISPs to curtail the bandwidth they allow OptIn, which in turn affects OptIn's ability to send out e-mails it is contractually obligated to send.

A. What is Spam

Spam is "unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups; junk e-mail." American Heritage Dictionary of the English Language, (4th ed. 2000). As much as 80 percent of the e-mail received through the nation's largest ISP, America Online, is spam. (Newby Decl., Exh. F.1, Newsday, *Junk Mail Joust* (June 22. 2003)) AOL filters 2.4 billion spams a day. (Id.) According to one consulting firm, coping with spam will cost U.S. companies more than $10 billion this year in cash wasted. (Id.) According to another research group, around $2 of the typical monthly Internet service bill goes toward fighting spam. (Id.)

A representative for Sonic.Net, an ISP, has complained that, "Spam consumes system resources such [as] disk storage space, processor cycles and bandwidth, which slows delivery of normal communications...and consumes, and in most cases wastes, the time and energy of network administrative personnel and users." (Cummins Decl. ¶ 4.) Mr. Cummins describes spam as a "pernicious problem for ISPs...[as it is] relatively inexpensive for the sender to send compared to the costs of printing and mailing paper advertisements, and yet imposes a heavy cost on ISPs and their customers who do not wish to

receive spam." (Id.) These costs include "[f]iltering incoming mail, protecting network security and clearing spam from users' email inboxes [which,] takes a significant amount of time and resources, including the time and energy of [an ISP's] staff of system administrators and purchase or development of spam filtering software tools." (Id.)

In response to these growing concerns regarding spam, in December 2003, Congress enacted the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, or the CAN-SPAM Act of 2003. Pub. L. 108-187 (Dec. 16, 2003) ("CAN-SPAM Act" or "the Act"). It took effect in January 2004. In enacting CAN-SPAM, Congress found that:

> The convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail. Unsolicited commercial electronic mail is currently estimated to account for over half of all electronic mail traffic, up from an estimated 7 percent in 2001, and the volume continues to rise. Most of these messages are fraudulent or deceptive in one or more respects.

CAN-SPAM Act, Pub. L. 108-187, § 2(a)(2).

Congress further found that " [t]he receipt of unsolicited commercial electronic mail may result in costs to recipients who cannot refuse to accept such mail and who incur costs for the storage of such mail, or for the time spent accessing, reviewing, and discarding such mail, or for both" and that spam "also decreases the convenience of electronic mail and creates a risk that wanted electronic mail messages, both commercial and noncommercial, will be lost, overlooked, or discarded amidst the larger volume of unwanted messages, thus reducing the reliability and usefulness of electronic mail to the recipient." CAN-SPAM Act, Pub. L. 108-187, § 2(a)(3)-(4).

Accordingly, "[t]he growth in unsolicited commercial electronic mail imposes significant monetary costs on providers of Internet access services, businesses, and educational and nonprofit institutions that carry and receive such mail, as there is a finite volume of mail that such providers, businesses, and institutions can handle without further investment in infrastructure." CAN-SPAM Act, Pub. L. 108-187, § 2(a)(6).

B. SpamCop

SpamCop is an interactive Internet-based service whose mission is to reduce spam by reporting complaints to ISPs that provide Internet access to the senders of spam ("spammers"). (Haight Decl. ¶¶ 2-3). Whereas many anti-spam companies provide filtering services, which blocks an anti-spam customer from receiving spam, SpamCop goes one step further. It forwards complaints to ISPs to encourage ISPs to sanction spammers, including cutting off the spammers bandwidth (e.g. their access to the Internet). (Haight Decl. ¶¶ 4-6). SpamCop's founder, Julian Haight, has stated that he has helped close many spammers' e-mail accounts. (Piepmeir Decl., Exh. A, New York Times, *To Protest Unwanted E-Mail, Spam Cop Goes to the Source* (June 24, 1999)).

1. How the SpamCop System Works

SpamCop's registered users forward what they believe to be spam to SpamCop. SpamCop determines the ISPs from which the alleged spam was sent, including the ISPs supporting banner ads that accompanied the spam. (Haight Decl. ¶ 4.) Typically, spammers are able to disguise their identity by, for example, using fictitious e-mail addresses, or ones that are closed within a short time after mailing. CAN-SPAM Act, Pub. L. 108-187, § 2(a)(7). SpamCop addresses this issue by using a combination of Unix utilities (the utilities employed by most e-mail systems) to cross-check all the information in an e-mail header and find the e-mail address of the administrator on the network where the e-mail originated. (Haight Decl., Exh. A, SpamCop.net: What is this? How does it work? How do I Use it?).

To find the originating ISP, SpamCop software breaks down the e-mail header into its component parts ("parsing"), and then runs a thorough search on the IP addresses to determine the originating network. (Haight Supp. Decl. ¶ 11.) A reported message may contain information in its headers indicating numerous potential sources. (Haight Supp. Decl. ¶ 12.) In some cases, the sender of bulk e-mails may send messages through multiple ISPs. (Id.) In those instances, SpamCop alleges that it is difficult to determine the exact originating ISP, and therefore, it forwards the complaint to all of the ISPs through which the message may have been sent. (Id.) Additionally, web site or banner advertisement links in the message may indicate the actual source that is responsible for the message. (Id.) For example, if a reported message contains a banner advertisement for "AcmeMortgages.com," it is possible that the entity that is ultimately responsible for the e-mail is AcmeMortgages.com. (Id.) In some circumstances, there are also

red herring links to websites in a report message that the senders include in an apparent effort to make it difficult for recipients and software like SpamCop's to determine the true source of the message. (Id.)

Once the IP addresses are parsed from the e-mails, SpamCop's system determines the address at an ISP to which the e-mail should be reported. (Haight Supp. Decl. ¶ 13.) SpamCop cross-checks the IP addresses in the message headers against numerous internal and online databases – including but not limited to SpamCop's internal database. (Id.) SpamCop uses a number of sources including default postmaster and abuse accounts maintained by the ISPs, a database maintained by Abuse.Net (an independent third party that tracks addresses at ISPs for the submission of e-mail abuse complaints), and routing information that SpamCop has gathered. (Id.) In addition, ISPs sometimes designate one or more individuals within their organization to whom complaints about spam may be directed. (Id.)

SpamCop's registered users who report purported spam may add comments to the report. (Haight Decl. ¶ 4.) When SpamCop forwards the user's complaint, it does not add any comments or criticism of its own. Instead, it states: "This message is brief for your comfort. Please follow links for details." (Haight Supp. Decl. ¶ 14.) An ISP administrator who clicks on the links will be sent to a page on SpamCop's website. On that page SpamCop explains to ISPs that it has tracked the source of purported spam to the ISP. While it encourages the ISP to take action against the spammer, it also cautions, "Please be careful when taking action. It is possible (though unlikely) that the account is what we call 'an innocent bystander.'" (Haight Decl., Exh. C, SpamCop.net: Introduction – What is this thing? How does it work?) SpamCop also states, "SpamCop administrators do not, and cannot verify the claims made by it's [sic] users. Not only are there simply far too many reports filed for anyone to manually review them, but even if it were to, there is no way for us to know whether a user actually did or did not solicit a message prior to reporting it as spam." (Id.) It also gives ISPs the option of not receiving these unsolicited reports.

2. Removal of the Registered User's Names

When it forwards the report to the ISPs, SpamCop removes the e-mail address of the registered user. (Haight Decl. ¶ 9.) Its purpose in doing so is to protect the privacy of the registered user. (Id.) SpamCop believes that if it did not remove the registered user's e-mail address, the registered user could be subjected to retaliatory actions, including hacking attacks or being flooded with spam. (Id.) Registered

users also prefer that their names be removed. (Block Decl. ¶ 10.)

SpamCop also admits, however, that it removes the names to preserve the efficacy of its business by preventing spammers form "list washing." (Id.) List washing is a process whereby spammers remove the very small percentage of people on their bulk lists that actually report spam. SpamCop believes that if spammers could target and selectively remove those persons reporting spam, they could evade detection and continue to send unsolicited bulk e-mail messages to other recipients. (Id.)

C. OptIn

OptIn states that it is not a spammer, but rather a sender of bulk commercial e-mails in compliance with federal laws. (Richter Decl. ¶ 2.) OptIn provides "opt-outs" on e-mails it sends, and it sends e-mails only to those Internet users who have directly opted-in, or indirectly opted-in by visiting a particular website. (Id.) OptIn contracts with ISPs to provide OptIn bandwidth so that it may meet its contractual terms to send e-mail advertisements on behalf of OptIn and its customers. (Richter Decl. ¶ 3.) It needs a great deal of bandwidth because it sends "millions" of e-mails each day. (Richter Decl. ¶ 2.)

OptIn is, however, the target of parallel suits by the Attorney General's Office of the State of New York and Microsoft Corporation for sending what these two plaintiffs describes as spam. (Newby Decl., Exh. C.) OptIn's founder, Scott Richter, has been described in various press reports as "the world's third-largest spammer." (Newby Decl., Exh. D.) Numerous other articles submitted by SpamCop also describe Mr. Richter and OptIn as spammers, responsible for billions of unsolicited bulk commercial e-mails. (Newby Decl. Exh. F.) In other words, SpamCop is not the only entity describing OptIn as a spammer.

OptIn's principle ISP is a company called Optigate. On or about April 29, 2004, Optigate informed Mr. Richter that its upstream provider, Above.net, had terminated some of Optigate's bandwidth because of OptIn's violations of Above.net's "Acceptable Use Policy" (which prohibits spamming). (Richter Decl. ¶ 10.) Above.net did not specifically state that the violations came to its attention through reports from SpamCop.

OptIn has been informed by Optigate that if it, or Above.net, continue to receive SpamCop reports regarding OptIn, they will be forced to terminate OptIn's bandwidth entirely. (Wolfe Decl. ¶ 4.) Other ISPs who provide OptIn with bandwidth have informed OptIn of the same. (Morrison Decl. ¶ 5.)

D. The Dispute Between SpamCop and Optin

OptIn alleges that SpamCop sends multiple copies of the same reports to ISPs, which inflates the actual number of reports against OptIn. In other words, one complaint becomes multiple complaints that cannot be distinguished because SpamCop has removed the registered user's e-mail address from the reports. (Wolfe Decl. ¶ 3.)

Officially, SpamCop discourages individuals from submitting more than one complaint regarding a single spam. (Haight Decl. ¶ 8.) SpamCop attempts to remove duplicative submissions and states that it takes corrective action against individuals who submit duplicate requests, up to and including banning complaints from individuals engaged in this practice. (Id.)

SpamCop further explains that it does not intentionally send multiple copies of the same complaint to the same ISP. Its software is not designed to do so. (Haight Supp. Decl. ¶ 20.) If the multiple copies are being sent, it is for one of three reasons. First, it may be because the ISP has directed that complaints be sent to more than one recipient within its system. (Haight Supp. Decl. ¶ 13.) Second, if the ISP supported both the e-mail and the banner ad, then SpamCop may report two issues, one that the purported spam passed through the ISP's network, and two that the ISP hosted a banner ad appearing in the purported spam. (Haight Supp. Decl. ¶ 16.) Finally, though SpamCop is not aware of any, multiple mailings may be caused by a bug in its program. (Haight Supp. Decl. ¶ 20.)

At the hearing, the parties disputed whether Exhibit B of the Wolfe Declaration proved that multiple copies of the same e-mail report were being sent to one ISP. OptIn's counsel, relying on hearsay, argued that the exhibit demonstrated that the same report had been sent multiple times. In his supplemental declaration, Mr. Haight has explained that this is not the case. (Haight Supp. Decl. 17.) The Court is satisfied by Mr. Haight's explanation of Exhibit B of the Wolfe Declaration. Exhibit B is a copy of a report that SpamCop sends to itself when its system identifies Internet access providers or linked advertisers in the spam, but does not republish the report to those entities.[1]

---

[1]The Supplemental Declaration of Doug Wolfe does little to refute Mr. Haight's explanation. Mr. Wolfe submits as Exhibit A what he claims is an example of how SpamCop sends the same report to numerous ISPs. Yet this Exhibit is a printout from SpamCop's own website, and as Mr. Haight has already explained,

On its website, SpamCop provides a link called "You are mailbombing me! How can I make it stop?" This link allows ISPs to change their preferences for receiving reports from SpamCop, request that SpamCop stop sending reports, or send only certain reports. (Haight Supp. Decl. ¶ 20.) SpamCop alleges that in April 2004, it received 89,000 reports of spam emanating from OptIn.

E. ISPs

SpamCop alleges that it is not responsible for the actions ISPs take once they receive the reports. Moreover, SpamCop argues, the ISPs do not rely on the reports alone to determine whether to sanction or terminate network access to a spammer. For example, a representative for the ISP Sonic states that although "Sonic welcomes the receipt of [SpamCop's reports], [they] are not the only source of data [ ] but instead are only a part of what we consider." (Cummings Decl. ¶ 5.) Sonic considers "other data, including but not limited to listings in various lists, newsgroups and mailing lists." (Cummings Decl. ¶ 6 .) Sonic also clarifies that it understands that SpamCop's "process of reporting suspected spam is automated." (Cummings Decl. ¶ 7.) Thus, Sonic "undertakes its own investigation to ensure that a flagged IP address is in fact conducting activity in violation of [Sonic's policy on spam]." (Id.)

OptIn counters that Sonic may be the exception, rather than the rule. The proprietor of Cheap Unix Hosting, for example, states that he has made the decision to terminate customers based solely on receiving SpamCop complaints. (Papadakis Decl. ¶ 2.) "This decision is based on the fact that if I do not terminate the customer who is the target of the SpamCop complaints, our upstream providers will terminate our services." (Id.)

The director of the ethical volume e-mailing company Hula Direct states that "[i]t has been my experience with [ISPs] that such providers rely heavily on complaints from SpamCop to make a determination of whether my company is in compliance with the [ISPs'] acceptable use policy and/or determine if my company is sending spam. At times [ISPs] will use SpamCop complaints exclusively to make this determination and to determine whether or not to shut off services to my company." (Warsinke Decl. ¶ 1.)

---

it is SpamCop's report to itself, not to third parties.

The managing partner of IPWS, LLC, an ISP states that "IPWS entered into a contract with [OptIn] to provide OptIn with bandwidth," but that he was notified by his upstream provider Qwest that they had received numerous SpamCop reports regarding OptIn and were "terminating their services to us that pertain to OptIn because of the number of SpamCop complaints they received." (Morrison Decl. ¶ 2; Morrison Decl. ¶ 3.)

From the facts in the record, at the very least, SpamCop's reports can strongly influence or play an important role in an ISP's decision to sanction senders, such as OptIn.

III. IMMUNITY

Before analyzing the merits of OptIn's preliminary injunction motion, the Court reviews the Communications Decency Act ("CDA") to determine whether SpamCop is immune.

A. Communications Decency Act

CDA § 230 provides, "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c)(1). The purpose of this section is "to maintain the robust nature of Internet communication and accordingly, to keep government interference in the medium to a minimum." Zeran v. America Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997). "Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium. The imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive government regulation of speech." Id. Through § 230, Congress "sought to prevent lawsuits from shutting down websites and other services on the Internet." Batzel v. Smith, 333 F.3d 1018, 1027-28 (9th Cir. 2003).

Thus, under § 230, interactive service providers and users cannot be held liable for the republication or redistribution of statements "provided by any other content provider." 47 U.S.C. § 23(c)(1). An "interactive computer service" is broadly defined as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server...." 47 U.S.C. § 230(f)(2). Courts construing § 230(f)(2) have recognized that the definition includes a wide range of cyberspace services, not only internet service providers. See, e.g., Blumenthal v.

Drudge, 992 F.Supp. 44 (D.D.C. 1998) (AOL is an "interactive computer service"); Gentry v. eBay, Inc., 99 Cal.App.4th 816, 831 & n. 7 (2002) (on-line auction website is an "interactive computer service"); Schneider v. Amazon.com, 108 Wash.App. 454, 31 P.3d 37, 40-41 (2001) (on-line bookstore Amazon.com is an "interactive computer service").

B. Where the CDA Applies

"[C]laims seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions – such as deciding whether to publish, withdraw, postpone or alter content – are barred." Carafano v. Metrosplash.com, Inc., 207 F. Supp. 2d 1055, 1064 (C.D.Cal. 2002). For example, America Online is a typical interactive computer service. Zeran, 129 F.3d at 329; Blumenthal, 992 F.Supp. at 50. In Blumenthal, a district court held that while America Online: (1) solicited a gossip report from author Matthew Drudge; (2) retained the right to modify or edit it (but declined to do so); (3) heavily advertised the report and encouraged people to becomes subscribers of AOL to access the report; (4) it was nevertheless immune from suit. All that America Online had done was republish the report. It was not responsible for its content.

In Batzel, the Ninth Circuit held that where: (1) a listserv moderator made minor edits to an e-mail he received; and (2) forwarded it to his automatic listserv; (3) he was immune from liability. Had he engaged in extensive or substantive editing, he could have been liable because then he would have altered the statements rather than merely redistributed them. Id.

Both the Blumenthal court and the Ninth Circuit have noted that any analogy between activities in the bricks and mortar (traditional, non-Internet) world and the Internet world will fail because Congress has distinguished the activities of the two. In Blumenthal, because AOL had the right to exercise editorial control, the court noted that had AOL's activity been limited to the bricks and mortar world, it would have likely found that AOL was indeed liable. As the Ninth Circuit has explained, "[t]he specific provisions at issue here, § 230(c)(1), overrides the traditional treatment of publishers, distributors, and speakers under statutory and common law." Batzel, 333 F.3d at 1026. This is because "[a]s a matter of policy, Congress decided not to treat providers of interactive computer services like other information providers such as newspapers, magazines or television and radio stations, all of which may be held liable for publishing or

distributing obscene or defamatory material written or prepared by others." Id. (internal quotations and citations omitted).

C. Where the CDA Does Not Apply

In contrast, where a service provider contributes to the content, then it is not immune. For example, in Carafano v. Metrosplash.com, 207 F. Supp. 2d 1055 (C.D.Cal. 2002), the defendant provided multiple-choice questions and a series of essay questions that shaped the eventual content that subscribers posted. This rendered the defendant "responsible...in part for the creation or development of information provided through the Internet...." Id. at 1066-1067.

In MCW, Inc. v. badbusinessbureau.com, 2004 WL 833595 (N.D.Tex. April 19, 2004), the defendants operated a web site that served in part as a consumer complaint forum. Not only did the defendants post consumer complaints, they organized them geographically by company and under various other headings including "Con Artists" and "Corrupt Companies." Id. at *9 fn. 10. Moreover, the defendants contributed to the content by instructing a consumer to take photos to include in his complaint that defendants then posted. Id. at *10. Thus, the defendants did not merely exercise the traditional rights of a publisher, they contributed to and shaped the content. Accordingly, they were not immune from liability. Id.

D. Distribution

The Courts review of the case law, supra, focuses on publication. In the case at hand, the parties agree that in addition to publishing the reports of registered users, SpamCop distributes them by forwarding copies of the reports to third parties who are not subscribers to SpamCop's services. Although the Ninth Circuit has not directly addressed the issue of distributors, it has observed that courts have consistently found that the CDA does not distinguish between publishers and distributors. Batzel, 333 F.3d at 1027 fn. 10 (and cases cited therein). "Congress made no distinction between publishers and distributors in providing immunity from liability." Blumenthal, 992 F.Suppp. at 52. "[I]f computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement – from any party, concerning any message." Zeran, 129 F.3d at 333.

Thus, the question becomes, under what circumstances is a distributor immune under the CDA?

The parties did not cite any authority that focused on distributors. The Court itself has not found any. Optin argues that the focus should be on the breadth of the distribution. In Blumenthal, AOL's activities were limited to subscribers. In Batzel, the listserv manager selected the particular e-mails to be published, which were then sent to subscribers of the listserv. In contrast, SpamCop sends its reports to non-subscribers. OptIn argues that deliberately sending the reports to non-subscribers, that is third parties who did not choose to receive the reports, removes SpamCop from immunity. In essence, OptIn is analogizing the act of editing so as to alter the content, which would remove a publisher from immunity, to the act of editing a distribution list to include non-subscribers.

There is no precedent, however, for such an analogy. The focus is not on the distribution list, it is on the content of the e-mail and the distributor's complicity in shaping that content. Moreover, the Court is not persuaded that sending reports to non-subscribers somehow affects the immunity of a distributor. Nor is it persuaded that Congress intended such distribution to affect immunity. Rather, Congress has chosen to provide "immunity even where the interactive service provider has an active, even aggressive role in making available content prepared by others." Blumenthal, 992 F.Supp. at 51-52. Distributing content to non-subscribers may be perceived as aggressive activity, but it does not destroy the distributor's immunity.

Reviewing the case law and the statute, it appears that the focus on distributor liability is and should be conterminous with the focus on publisher liability: content. Just like a publisher, if a distributor alters the content, then the distributor may be liable. For example, the Carafano court noted that because it had found that the defendant was liable for altering the content, it did not need to reach the question of whether the defendant was also liable as a distributor for defamation. 207 F.Supp. at 1074-75. Because the defendant created and tailored membership questionnaires that helped to create the subsequent content, the defendant was not just a passive conduit of information. It was a contributor to the content.

E. Whether SpamCop has Contributed to the Content

Thus, to determine whether or not SpamCop is immune, the Court must determine whether SpamCop has contributed to the content. OptIn argues that SpamCop has contributed to the content of the reports in two ways. First, it has included information in the reports. Second, by sending out numerous reports, it affects the impact of the reports.

With respect to content, unlike the defendants in MCW, Inc. v. badbusinessbureau.com, SpamCop does not organize the reports with headings or other matter. Unlike the defendants in Carafano, SpamCop has not created questionnaires or other forms that registered users use in shaping the content of the reports.

Instead, when SpamCop sends out the reports, it removes the registered user's name and includes the following statement: "This message is brief for your comfort. Please follow links for details." The links lead a recipient back to SpamCop's website, where SpamCop explains its business, provides an opt-out, and cautions that it cannot guarantee the veracity of the report. These activities cannot be considered a contribution to the content. They do not alter, shape, or even edit the content. SpamCop's activities are even more innocuous than, for example, the activity and addition that the defendant in Batzel provided. In Batzel, the defendant provided minor edits to the actual content; he also stated in the republication that a copy of the original e-mail had been sent to the authorities. The Ninth Circuit held that such activity did not "rise to the level of development" because it did not alter the basic form and message of the original e-mail. Batzel at 1031.

With respect to the impact, it may be true that SpamCop is aggressive in mailing the reports to any and all ISPs that it can identify in the mailing header of the purported spam. OptIn has failed to show, however, that SpamCop sends multiple copies of the same report to the same recipient in order to inflate its impact. Even if OptIn had, the Court is not persuaded that multiple mailings would amount to an alteration in the content found within each report. The content of each republished report remains the same and a recipient may identify them as multiple copies of the same report. In addition, in terms of the traditional role of a distributor, the Court perceives no substantive difference between distributing one copy of an item once, and distributing the same item numerous times.

F. Summary

SpamCop is an interactive service provider, like web sites such as Amazon.com. It uses interactive computer services to distribute its on-line mailing and to post the reports on its website. See Batzel at 1031 (describing characteristics of an interactive service provider for CDA immunity). It collects reports from registered users. It posts them on its website. It sends copies of the reports to non-subscribers. It may be aggressive in its mailings, but SpamCop has not altered the content of the messages and thus, under the

CDA it is immune from liability. For this reason alone, the Court DENIES OptIn's motion for a preliminary injunction. For the sake of thoroughness, however, the Court sets out in Section IV, infra, the reasons why even if SpamCop were not immune from liability, OptIn's motion for preliminary injunction would nevertheless fail.

IV. PRELIMINARY INJUNCTION

OptIn has requested that the Court issue a preliminary injunction enjoining SpamCop from: (1) making any slanderous or libelous statements pertaining to OptIn; (2) directly or indirectly transmitting or sending reports it forwards to third parties regarding OptIn to anyone other than OptIn's originating ISP; (3) removing the e-mail addresses from reports it receives regarding OptIn; and (4) otherwise engaging in the unlawful conduct set forth in the Complaint.

From the outset, it should be clear that the first and last request are too broad and too vague for a preliminary injunction. "Any slanderous or libelous statement" could include a statement regarding the pending suit, other suits pending against OptIn, or past criticism of OptIn. "Otherwise engaging in unlawful conduct set forth in the Complaint" presumes that the Complaint sets forth unlawful conduct and imposes a judgment against SpamCop even before a judgment has been rendered. Thus, the only two activities the Court considers in regards to an injunction are the second (transmitting reports to third parties other than OptIn's originating ISP) and the third (removing e-mail addresses from reports it receives).

A. Legal Standard

In the Ninth Circuit, two interrelated tests exist for determining the propriety of the issuance of a TRO or preliminary injunction. Under the first test, the Court may not issue a preliminary injunction unless: (1) the moving party has established a likelihood of success on the merits; (2) the moving party will suffer future irreparable injury and has no adequate remedy at law if injunctive relief is not granted; (3) the balance of hardships tips in favor of the movant; and (4) granting the injunction is in the public interest. Martin v. International Olympic Committee, 740 F.2d 670, 674-75 (1984). An alternative articulation of the test is whether the moving party "meet[s] its burden by demonstrating either a combination of probable success on the merits and the possibility of irreparable injury or that serious questions are raised and the balance of hardships tips sharply in its favor." Martin, 740 F.2d at 675. The two tests are not, however, separate and

unrelated; they represent the "extremes of a single continuum." Benda v. Grand Lodge of Int'l Ass'n of Machinists, 584 F.2d 308, 315 (9th Cir.1978).

B. Likelihood on the Merits

OptIn bases its preliminary injunction on: trade libel, intentional interference with contractual relations and unfair competition.

1. Trade Libel

To prevail in a claim for trade libel, a plaintiff must demonstrate that the defendant: (1) made a statement that disparages the quality of the plaintiff's product; (2) that the offending statement was couched as fact, not opinion; (3) that the statement was false; (4) that the statement was made with malice; and (5) that the statement resulted in monetary loss. Guess, Inc. V. Superior Court, 176 Cal.App.3d 473, 479 (1986).

OptIn asks the Court find that: (1) SpamCop's sending of the same report to not just OptIn's originating ISP, but to any ISP to which SpamCop can trace the alleged spam is a statement that disparages OptIn; (2) that the accusation of spam is couched as fact; (3) that by virtue of the mailing of one report to numerous ISPs, SpamCop inflates the actual number of reports against OptIn which results in a falsity; (4) that there is malice in that SpamCop's very purpose is to shut down senders of bulk commercial e-mails whether they be legitimate or not; and (5) OptIn has had its bandwidth reduced by Optigate and its bandwidth cut by IPWS.

First, the Court questions whether SpamCop's reports can be deemed to be couched as fact when SpamCop informs the ISPs that it cannot verify the reports. SpamCop does not represent that the reports are of spam, or that the registered user opted-out of the OptIn mailings and nevertheless continued to receive the mailings.

Second, with respect to the issue of falsity, the Court questions whether SpamCop sends the same report several times to the same ISP. OptIn has not demonstrated that it does. OptIn also alleges that by sending the reports to all of the ISPs on the mailing header, which includes the upstream and downstream ISPs, SpamCop creates a falsity by inflating the number of reports against it. The Court questions, however, whether SpamCop can be held responsible for an upstream ISP's determination to cut bandwidth

when it knows that reports sent to both it and its downstream ISP may be duplicative. It would seem that given the industry knowledge about SpamCop, ISPs must make their own determination as to what weight, if any, they will give SpamCop's reports.[2]

Setting aside these questions, though, OptIn still faces a fundamental hurdle in its claim for trade libel – malice. It has not submitted any evidence that SpamCop has particular malice towards it. Without even a hint of malice, it is difficult to say that OptIn has a likelihood of prevailing on the merits of its trade libel claim.

2. Interference with Contractual Relations

To prevail on a claim for interference with prospective economic advantage, a plaintiff must prove: (1) the existence of an economic relationship between the plaintiff and a third party; (2) that the defendant was aware of the relationship and acted wrongfully with the purpose of disrupting the relationship; (3) that the relationship was disrupted; and (4) that the plaintiff suffered damages that flow proximately from the disruption. Lowell v. Mother's Cake & Cookie Co., 79 Cal.App.3d 13, 17 (1978). The wrongful act must be "conduct that was wrongful by some legal measure other than the fact of interference itself." Tuchscher Development Enterprises, Inc. V. San Diego Unified Port Dist., 106 Cal.App.4th 1219, 1242 (2003).

Here, OptIn's claim falters on the second issue – that SpamCop's interference was actually wrongful. OptIn has not demonstrated that SpamCop's sending the reports to ISPs is wrongful by some legal measure.

---

[2]Notably, the supplemental declarations that OptIn sought to include underscores the fact that ISPs determine the amount of weight to be given SpamCop's reports and that the industry understands that SpamCop's reports cannot be verified. For example, Mr. Ray Everett-Church puts himself forward as an industry expert and a member of the Coalition Against Unsolicited Commercial Email. (Everett-Church Decl. ¶ 2.) He declares, "the lack of objective criteria and the apparently low threshold of complaints needed to be placed on their 'blocklist,' combined with the fact that anyone can submit a complaint about emails they receive whether or not the email was actually spam, can result in a high false-positive rate for declaring a particular email service provider to be a source of 'spam.'" (Everett-Church Decl. ¶ 7.) His statement reflects industry knowledge regarding the limitations of SpamCop's reports. Thus, a particular ISP's decision to give more weight to SpamCop's reports than they may merit is the fault of the ISP, not SpamCop.

Because the Court strikes OptIn's supplemental declarations, the Court did not consider Mr. Everett-Church's declaration in rendering this decision.

At the hearing, OptIn argued that the actual wrong arose from SpamCop misleading ISPs by inflating the number of reports. OptIn, however, failed to prove that SpamCop actually sends numerous copies of the same report to the same ISP or that the result of such mailings is that ISPs mistakenly believe that the reports are from numerous registered users, rather than one.

At the hearing, OptIn also argued that the multiple mailings have harmed OptIn's reputation because third party ISPs are now less likely to contract with OptIn to provide bandwidth. This, however, must be countered by the numerous news articles that clearly establish that OptIn's reputation as a spammer precedes it. It is being sued by the state of New York and Microsoft Corporation. It has been described as a spammer in numerous press articles and it has been found by one Internet analysis group to be the third largest spammer in the world.

Moreover, to the degree that SpamCop's practice does inflate the number of actual reports or otherwise harms OptIn's reputation, it is the ISPs themselves who allow SpamCop's reports to impact their perception of OptIn and affect their decision making. Whether they choose to rely entirely on SpamCop's reports, or ignore them, or to conduct some investigation on their own, it is the ISPs who ultimately make the decision whether or not to terminate OptIn's bandwidth. In addition, because SpamCop reproduces the purported Spam in full, the ISPs can actually determine for themselves whether or not OptIn has complied with CAN-SPAM by providing a valid and functioning opt-out link.

Again, based on the record, OptIn has not established that it is likely to prevail on its claim of interference with prospective economic advantage.

3. Unfair Business Practices

OptIn alleges that SpamCop's activities amount to unfair business practices because despite OptIn's numerous attempts to persuade SpamCop to provide the e-mail addresses of the registered users in order to that OptIn can correct its bulk list servers, SpamCop has refused to cooperate.

To be specific, CAN-SPAM regulates the activities of senders of bulk commercial e-mails. It requires that unsolicited messages contain certain minimum elements such as a valid and functioning return address, a "clear and conspicuous" identifier that the message is an advertisement or solicitation, a means for the recipient to opt-out, a valid physical postal address of the sender, and warning labels on e-mail

containing sexually oriented material. CAN-SPAM Act, Pub. L. 108-187, Sec. 5. It imposes penalties on those senders who, for example, fail to include these elements, or fail to honor opt-out requests. CAN-SPAM Act Pub. L. 108-187, Sec. 4-5.

OptIn alleges that it provides opt-out links and honors opt-out requests. It is concerned that the registered users who are sending reports to SpamCop represent people whose opt-out requests have failed for some reason. It believes that it needs the e-mail addresses of those users in order to take corrective action to delete them from its bulk lists. If these registered users have opted-out, but the opt-out has failed and OptIn continues to send them e-mails, OptIn will be in violation of CAN-SPAM and subject to fines.

OptIn has utterly failed to identify any law that would require SpamCop to divulge these e-mail addresses. In a way, OptIn's request is analogous to one who either intentionally or unintentionally sends pornography to minors, who then asks for a list of those minors so he will not continue to commit the crime. The responsibility for complying with the Act and preventing the violations begins and ends with OptIn.

C. Serious Questions

OptIn has not demonstrated a likelihood of success on the merits. The Court has found that SpamCop is immune under the CDA. Nevertheless, to be thorough, the Court reviews the other half of the sliding scale: whether OptIn has raised serious questions going to the merits and demonstrated the possibility of irreparable harm.

D. Irreparable Harm

An irreparable harm is one that cannot be redressed by a legal or equitable remedy following trial. Public Util. Comm'n v. FERC, 814 F.2d 560, 562 (9th Cir.1987) OptIn alleges that it will suffer damage to the goodwill of its business, damage to contract rights, and damage to the existence of its business.

Damage to a business' goodwill is typically an irreparable injury because it is difficult to calculate. Rent-A-Center, Inc. V. Canyon Television & Appliance Rental, Inc., 944 F.2d 597, 603 (9th Cir. 1991). It is true that when SpamCop sends out reports to ISPs, these reports affect OptIn's reputation and goodwill. This does not mean, however, that SpamCop is fully responsible for any damage these reports make to OptIn's goodwill. First, there is the fact that OptIn's reputation precedes it. Second, SpamCop cannot be held entirely responsible for the decisions these ISPs make. These ISPs may be more likely to

assume that OptIn is a spammer because they are already aware of OptIn's reputation. Thus, it would take fewer reports to persuade these ISPs to terminate OptIn's bandwidth.

The Second Circuit has found that where wrongful conduct deprives a plaintiff of a unique contract right, there may be an irreparable harm. Reuters Ltd. V. United Press Int'l, Inc., 903 F.2d 904, 908-909 (2nd Cir. 1990). OptIn's bandwidth has been diminished by one ISP and completely terminated by another. If the Court found SpamCop's activity to be wrongful, or that there were serious questions regarding SpamCop's activity, then the loss of bandwidth could be an irreparable harm.

Irreparable harm is further found where the conduct of a defendant threatens the existence of the business itself. Petereit v. S.B. Thomas, Inc., 63 F.3d 1169, 1186 (2nd Cir. 1995). The more ISPs that refuse to provide OptIn bandwidth, the less able OptIn will be to send out bulk commercial e-mails, whether they comply with federal law or not.

In short, OptIn has demonstrated that it is likely to suffer harm. The degree to which this harm is attributable to SpamCop is unclear, especially because part of the harm has been created by OptIn's own reputation independent of SpamCop. Moreover, to the degree that OptIn does suffer harm, such as being cut-off from bandwidth, the harm seems to emanate not from any act by SpamCop, but by the individual decisions of ISPs to allot great weight to SpamCop's reports without undertaking any investigation of their own.

E. Balance of Hardships

Assuming that OptIn faces irreparable harm, the Court must balance that harm on the one hand, with the balance of hardships on the other.

OptIn argues that in contrast to the irreparable harm it will face, the hardships to SpamCop if an injunction issues are minimal at best. It is not requesting that SpamCop cease its business operations. It is simply requesting that SpamCop send the reports only to OptIn's original ISP and that it provide OptIn with the e-mail addresses of the registered users who filed the reports.

With respect to the first request, SpamCop has explained that with some e-mails, it is impossible to determine the original ISP. Moreover, it has explained that its software does not distinguish between an "original" ISP and downstream or upstream ISPs. Requiring SpamCop to limit its distribution would

require SpamCop to alter its software. This creates a hardship on SpamCop.

With respect to the second request, the Court is quite wary that requiring SpamCop to provide the e-mail addresses of the registered users would have a chilling effect. Registered users concerned about retaliatory actions or loss of privacy would be less likely to post reports. The Court must balance this chilling effect and the public interest in free speech on the one hand, with OptIn's obligations under CAN-SPAM and the public's interest in its compliance with that Act. Although OptIn has not demonstrated that SpamCop is under a legal duty to provide OptIn these e-mail addresses, OptIn alleges that if it does not have them, then it is at risk of violating CAN-SPAM. Then again, it is OptIn's responsibility to ensure that its own opt-out procedures work, no one else's. Quite simply, the public's interest in protecting privacy and free speech outweigh whatever risks OptIn faces from its own faulty programming.

V. CONCLUSION

Based on the foregoing,

IT IS HEREBY ORDERED THAT OptIn's motion for a preliminary injunction is DENIED. Pursuant to § 230 of the Communications Decency Act, SpamCop is immune from liability for publishing or distributing the reports of registered users. Even if SpamCop were not immune, OptIn has failed to demonstrate that it is likely to prevail on the merits or that the balance of hardships tips in its favor.

IT IS FURTHER ORDERED THAT SpamCop's motion to strike the May 25 Pleadings is GRANTED.

IT IS SO ORDERED.

Dated: June 25, 2004

/s/ Saundra Brown Armstrong
SAUNDRA BROWN ARMSTRONG
United States District Judge