

Priority ~~_____~~
Send ~~_____~~
Enter ~~_____~~
Closed ~~_____~~
JS-5/JS-6 NO
JS-2/JS-3 _____
Scan Only _____

FILED
CLERK, U.S. DISTRICT COURT
JUL -2 2007
CENTRAL DISTRICT OF CALIFORNIA
BY DA DEPUTY

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
WESTERN DIVISION

ENTERED
CLERK, U.S. DISTRICT COURT
JUL 3 2007
CENTRAL DISTRICT OF CALIFORNIA
DEPUTY

12 MYSPACE, INC.,
13 Plaintiff,

14 v.

15 SANFORD WALLACE D/B/A
16 FREEVEGASCLUBS.COM, REALVEGAS-
17 SINS.COM, FEEBLEMINDED
18 PRODUCTIONS,

19 Defendant.

CV 07-1929 ABC (AGRx)

ORDER GRANTING IN PART
PLAINTIFF'S MOTION FOR
PRELIMINARY INJUNCTION

THIS CONSTITUTES NOTICE OF ENTRY
AS REQUIRED BY FRCP RULE 77(G)

21 On June 11, 2007, Plaintiff MySpace, Inc. ("Plaintiff") filed the
22 instant motion for a preliminary injunction. Defendant Sanford
23 Wallace d/b/a freevegasclubs.com, realvegas-sins.com, and Feebleminded
24 Productions ("Defendant") opposed on June 20, 2007, and Plaintiff
25 replied on June 27, 2007. The hearing on this matter was held on July
26 2, 2007. Based on the arguments of the parties and the pleadings in
27 this case, the Court hereby GRANTS IN PART Plaintiff's motion for a
28 preliminary injunction.

53

SCANNED

1
2 **I. STATEMENT OF FACTS**

3 Plaintiff is a "social networking service" that allows members to
4 create unique personal profiles online to find and communicate with
5 other people. (Declaration of Sarah Kaleel ("Kaleel Decl.") ¶ 3.)
6 Plaintiff provides its members with access to the MySpace.com website
7 and the MySpace.com instant messenger and to other Internet-based
8 features, content, and applications offered by Plaintiff in connection
9 with the MySpace.com website. (Id.) Users also have the ability to
10 send and receive communications to and from other MySpace.com users,
11 create groups, and post comments on bulletins. (Id.) To become a
12 member of MySpace.com, a user must create a profile by inputting his
13 or her name, country, zip code, birth date, and gender, must create a
14 password, and must provide an alternate email address to which
15 confirmations and notifications can be sent. (Id. ¶ 4.) Moreover,
16 when registering a user must agree with the Terms of Use Contract (the
17 "TOU Contract") by clicking an "I accept" button and inputting a
18 verification code, a unique series of letters and numbers designed to
19 prevent the use of automated processes to create profiles. (Id.) To
20 access a profile and message inbox, a user must log onto MySpace.com
21 or log on to his or her individual MySpace.com page via an individual
22 Uniform Resource Locator ("URL"). (Id.)

23 Plaintiff has expended significant time and resources in
24 implementing various measures to prevent abuse of its service and
25 curtail commercial spam (mass mailing of unsolicited commercial
26 email), including limiting the number of messages that can be sent
27 from a single MySpace.com account in a single day and using
28 sophisticated algorithms to identify potential spammers. (Id. ¶ 12.)

SWAMP
CALLE

1 Limiting spam is important because it clogs networks, uses up
2 bandwidth, and degrades the user experience. (Id. ¶ 11.)

3 Plaintiff claims that Defendant has engaged in an abusive multi-
4 faceted scheme to disseminate commercial messages and solicitation to
5 MySpace.com users. Defendant admits that he maintains two websites,
6 freevegasclubs.com and real-vegas-sins.com (the "Wallace Websites").
7 (Declaration of Sanford Wallace ("Wallance Decl.") ¶ 3.) In October
8 2006, Plaintiff's abuse team began receiving complaints related to the
9 Wallace Websites and after investigating, it discovered that Defendant
10 had created more than 11,000 similar MySpace profiles and 11,383
11 unique America Online email accounts to register those profiles.
12 (Kaleel Decl. ¶¶ 16-17.) Because an individual could not easily
13 create this number of unique profiles and because the naming
14 conventions used to create each profile and email address were
15 consistent, the abuse team concluded that Defendant must have used an
16 automated "bot" to register these profiles and addresses. (Id. ¶
17 18.)¹ The abuse team concluded that, by creating more than 11,000
18 unique email addresses, Defendant circumvented Plaintiff's unique-
19 email-address registration requirement and by creating 11,000 unique
20 profiles, Defendant circumvented Plaintiff's daily limit on the number
21 of messages that can be sent from any one profile in a single day.
22 (Id. ¶ 19.)

23 Plaintiff accuses Defendant of first sending out a series of
24 messages, comments, and bulletins to MySpace users designed to

25
26 ¹For example, 2,077 of Defendant's MySpace profiles were named
27 "What Pic Should I Upload?" and Defendant's AOL email addresses all
consisted of a 10- or 11-digit number followed by "@aol.com." (Kaleel
Decl. ¶¶ 16-17.)

1 redirect users to a website containing a MySpace.com logo and
2 soliciting the member's MySpace.com username and password through a
3 box that closely resembled the box used by members when logging onto
4 MySpace.com. (Declaration of Rick Frazier ("Frazier Decl.") ¶¶ 5-6.)
5 Defendant used this technique (called "phishing") to "hijack" members'
6 usernames and passwords so he could then log onto those other members'
7 MySpace.com profiles and send messages to those users' "friends,"
8 directing them to the Wallace Websites. (Id. ¶ 7.) In total,
9 Defendant sent nearly 400,000 messages and posted 890,000 comments
10 from 320,000 "hijacked" MySpace.com user accounts. (Id. ¶ 7, 13.)
11 Defendant also created "groups" on MySpace.com redirecting users to
12 the Wallace Websites, including altering the MySpace "unsubscribe"
13 link to point to the Wallace Websites rather than to actually allow
14 members to unsubscribe, and he used software code to lay graphics
15 containing links to the Wallace Websites over users' MySpace.com
16 profiles. (Id. ¶ 11-12.)

17 Plaintiff claims it has been harmed by Defendant's activity,
18 including incurring bandwidth and delivery-related costs, costs
19 associated with devoting time, money, and resources to stop
20 Defendant's activities, and harm to its reputation from 800 complaints
21 lodged by users over Defendant's activities. (Kaleel Decl. ¶¶ 20-21;
22 Frazier Decl. ¶ 15.) The Wallace Websites also contain adult
23 material, and since Plaintiff allows users as young as fourteen years
24 old to create profiles, Defendant's activities on MySpace.com create
25 the possibility that minors might view this offensive content.
26 (Frazier Decl. ¶ 8, Exh. G; Kaleel Decl. ¶ 14.)
27
28

II. LEGAL STANDARD FOR A PRELIMINARY INJUNCTION

To obtain a preliminary injunction, a plaintiff must show "either: (1) a likelihood of success on the merits and the possibility of irreparable injury; or (2) that serious questions going to the merits were raised and the balance of hardships tips sharply in its favor." Walczak v. EPL Prolong, Inc., 198 F.3d 725, 731 (9th Cir. 1999). "These two alternatives represent extremes of a single continuum, rather than two separate tests." Id. (internal quotations omitted). "Thus, the greater the relative hardship to [a plaintiff], the less probability of success must be shown." Id.; see also International Jensen, Inc. v. Metrosound U.S.A., Inc., 4 F.3d 819, 822 (9th Cir. 1993). Moreover, "[t]he district court must also consider whether the public interest favors issuance of the injunction." Southwest Voter Registration Educ. Project v. Shelley, 344 F.3d 914, 917 (9th Cir. 2003). A preliminary injunction is an "extraordinary remedy" for which the need must be "clear and unequivocal." Shelton v. National Collegiate Athletic Ass'n, 539 F.2d 1197, 1199 (9th Cir. 1976).

III. EVIDENTIARY OBJECTIONS

Plaintiff has objected to the entire declaration of Defendant's purported expert, Dr. Lawrence H. Miller. Miller's declaration purports to give legal conclusions on the interpretation of the statutes at issue in the Complaint, which is an impermissible subject for expert testimony. See Crow Tribe of Indians v. Racicot, 87 F.3d 1039, 1045 (9th Cir. 1996) ("Expert testimony is not proper for issues of law."); Mukhtar v. California State Univ., Hayward, 299 F.3d 1053, 1066 n.10 (9th Cir. 2002) ("[A]n expert witness cannot give an opinion

CONFIDENTIAL

1 as to her *legal conclusion*, i.e., an opinion on an ultimate issue of
 2 law." (emphasis in original)). Moreover, Miller has not testified to
 3 any foundational knowledge of how MySpace.com works, and even
 4 mistakenly opines that MySpace.com users can only send messages to
 5 users on their "friends" list, which Plaintiff has persuasively
 6 demonstrated is simply incorrect. (Declaration of Aber Whitcomb
 7 ("Whitcomb Decl.") ¶ 8.) Finally, Miller is qualified only to testify
 8 as an engineer at an aerospace corporation, and yet he offers opinions
 9 on advertising issues, consumer perceptions, and social networking
 10 sites such as MySpace.com, areas in which he has no apparent
 11 qualifications. His testimony on these points is not reliable as
 12 required by Kumho Tire Co. v. Carmichael, 526 U.S. 137, 149 (1999).
 13 Therefore, the Court sustains Plaintiff's objections to the Miller
 14 Declaration and will accord his testimony no weight.

15 The Court has also reviewed and considered all other evidentiary
 16 objections to facts on which the Court has relied, and hereby
 17 overrules those objections.

18 **III. ANALYSIS**

19 Plaintiff seeks a preliminary injunction based on violations of
 20 the CAN-SPAM Act, 15 U.S.C. §§ 7704(a)(1), (a)(3), (a)(5) and (b)(2),
 21 and violations of Cal. Bus. & Prof. Code § 17529.5, §§ 22984 et seq.,
 22 §§ 17200 et seq., and §§ 17500 et seq. As discussed below, the Court
 23 finds that Plaintiff has demonstrated a likelihood of prevailing on
 24 the merits of its claims under section 7704(a), so the Court need not
 25 determine whether Plaintiff will also prevail on its state-law claims.

26 **A. Likelihood of Success on the Merits.**

27 The CAN-SPAM Act, 15 U.S.C. §§ 7701 et seq. (the "Act"),

1 regulates the manner in which commercial email is transmitted and
2 regulates various activities related to commercial email, such as
3 prohibiting the use of false, misleading, or deceptive information,
4 prohibiting the use of automated "bots" to create multiple email
5 accounts, and requiring certain contact information in commercial
6 electronic mail messages. 15 U.S.C. § 7704(a)(1), (a)(3), (a)(5),
7 (b)(2). An "Internet access service" provider may seek to enjoin
8 conduct prohibited by sections 7704(a)(1) and 7704(b), or enjoin a
9 "pattern or practice" that violates section 7704(a)(2)-(5) and may
10 seek either actual or statutory damages, whichever is greater. Id. §
11 7706(g)(1), (3). However, because section 7704 is limited to
12 regulating only "commercial electronic mail messages," Plaintiff's
13 private right of enforcement exists only if Defendant's messages fall
14 within this statutory definition.

15 In opposition to Plaintiff's claims under the Act, Defendant
16 first argues that messages sent from MySpace.com member accounts do
17 not qualify as "electronic mail messages" as defined in the Act, and
18 therefore, Defendant cannot be liable under any of the Act's
19 provisions. The Act defines an "electronic mail message" as "a
20 message sent to a unique electronic mail address." Id. § 7702(6). An
21 "electronic mail address" is "a destination, commonly expressed as a
22 string of characters, consisting of a unique user name or mailbox
23 (commonly referred to as the 'local part') and a reference to an
24 Internet domain (commonly referred to as the 'domain part'), whether
25 or not displayed, to which an electronic mail message can be sent or
26 delivered." Id. §7702(5). A "domain name" is "any alphanumeric
27 designation which is registered with or assigned by any domain name

1 registrar, domain name registry, or other domain name registration
2 authority as part of an electronic address on the Internet." Id. §
3 7702(4).

4 Defendant argues that MySpace.com messages do not fall within the
5 Act's definitions of "electronic mail message" and "electronic mail
6 address" because the addresses to which those messages are sent lack a
7 "domain name" and have no route, instead remaining within the
8 MySpace.com system. The Court rejects these contentions. The Court
9 must assume that Congress expressed the legislative purpose of a
10 statute through the ordinary meaning of the words used. See Leisoni,
11 Inc. v. Stratman, 154 F.3d 1062, 1066 (9th Cir. 1998). The plain
12 language of the definition of "electronic mail address" entails
13 nothing more specific than "a destination . . . to which an electronic
14 mail message can be sent," and the references to "local part" and
15 "domain part" and all other descriptors set off in the statute by
16 commas represent only one possible way in which a "destination" can be
17 expressed. Indeed, the word "commonly" precedes the description of an
18 address with a domain part and local part, indicating that this
19 formulation is only one among many possible examples, rather than the
20 exclusive way in which the Act recognizes the expression of an
21 address. As Defendant himself points out, at the time the Act was
22 passed in 2003, electronic messages could be sent in many ways,
23 including through "instant messaging," and the Court must presume that
24 Congress was well-aware of these various forms of electronic
25 communications when it drafted the Act. The plain language of
26 "electronic mail address" encompasses these alternate forms while also
27 recognizing that the most commonly used form of electronic address was

1 the traditional "email" address with a local part and domain part
2 (i.e., "user@domain.com"). This expansive interpretation of the Act
3 supports the stated purpose of the Act, namely, curtailing the rapid
4 and detrimental growth of commercial electronic mail that has
5 overburdened electronic mail systems. 15 U.S.C. § 7701(a); see
6 MySpace, Inc. V. The Globe.com, Inc., Case No. 06-3391, 2007 WL
7 1514783, *4 (C.D. Cal. February 27, 2007) ("[T]he overarching intent
8 of this legislation is to safeguard the convenience and efficiency of
9 the electronic messaging system, and to curtail overburdening of the
10 system's infrastructure."). To interpret the Act in the limited
11 manner as advocated by Defendant would conflict with the express
12 language of the Act and would undercut the purpose for which it was
13 passed.

14 Even under Defendant's more restrictive interpretation, however,
15 messages sent through MySpace.com fall within the definition of
16 "electronic mail message" sent to an "electronic mail address." Each
17 MySpace.com user's mail resides on a unique URL, which includes a
18 string of characters containing the member's username and a reference
19 to the domain "myspace.com." (Whitcomb Decl. ¶ 4.) MySpace.com
20 messages also contain header information, such as source, destination,
21 and routing information, and references to the unique username and the
22 myspace.com domain name. (Id. ¶ 5.) As the court in MySpace, Inc.
23 aptly stated in response to this precise argument, "[w]hile the
24 routing employed by MySpace may be less complex and elongated than
25 those employed by traditional [Internet service providers], any
26 routing necessarily implicates issues regarding volume of traffic and
27 utilization of infrastructure -- issues which CAN-SPAM seeks to

1 address." 2007 WL at *5. Therefore, even under Defendant's unduly
2 narrow interpretation, each MySpace.com message qualifies as an
3 "electronic mail message" sent to an "electronic mail address."
4 Plaintiffs may properly bring suit under the Act against Defendant.

5 a. § 7704(a)(1)

6 Section 7704(a)(1) prohibits the use of false or misleading
7 header information, including header information that is "technically
8 accurate but includes an originating electronic mail address, domain
9 name, or Internet Protocol address the access to which for purposes of
10 initiating the message was obtained by means of false or fraudulent
11 pretenses or representations." 15 U.S.C. § 7704(a)(1)(A). "Header
12 information" is defined as "the source, destination, and routing
13 information attached to an electronic mail message, including the
14 originating domain name and originating electronic mail address, and
15 any other information that appears in the line identifying, or
16 purporting to identify, a person initiating the message." Id. §
17 7702(8). Plaintiff need not demonstrate a "pattern or practice" to
18 bring a claim under this subsection. Id. § 7706(g)(1).

19 Plaintiff argues that Defendant violated this subsection by
20 obtaining 342,000 MySpace.com members' usernames and passwords through
21 the Wallace Websites that misleadingly and falsely resembled the log-
22 in page at MySpace.com. He then used this information to log into
23 those members' accounts and send 400,000 spam messages from those
24 accounts to other users. Plaintiff also argues that Defendant falsely
25 obtained over 11,000 "dummy" MySpace.com profiles to spam other
26 members, collect members' personal information, send commercial
27 messages, and post prohibited content, all in violation of the TOU

1 Contract. Defendant claims that these allegations do not relate to
2 "headers" as required by this subsection, and even if they did, the
3 header information could not be altered or faked, so all the header
4 information was accurate. Further, Defendant argues that a
5 MySpace.com member cannot "arbitrarily" send out messages, but rather
6 each recipient must be on that member's "friends" list, making it
7 impossible for Defendant to violate this subsection.

8 Defendant is correct that, whatever the means by which he created
9 11,000 MySpace.com profiles, this activity, in itself, did not involve
10 sending messages with header information and does not implicate
11 section 7704(a)(1). The 400,000 messages Defendant sent via 340,000
12 other members' profiles, however, clearly violated this subsection.
13 In section 7704(a)(1)(A), Congress intended to prohibit not only
14 sending messages with inaccurate header information, but also sending
15 messages with accurate header information, access to which was
16 obtained through false or fraudulent pretenses. See Sen. Rep. No.
17 108-102 at 17 (2003) (stating that one purpose of section
18 7704(a)(1)(A) "is to eliminate the use of inaccurate originating email
19 addresses that disguise the identities of the senders."). Here,
20 Defendant obtained access to other members' usernames and passwords by
21 creating websites that appeared nearly identical to the log-in page at
22 MySpace.com. (Frazier Decl. ¶¶ 7-8, Exh. E.) He then used that
23 information to "hijack" 340,000 member accounts to send out mass
24 commercial messages. This clearly falls within the category of
25 messages prohibited where the header might be accurate but access to
26 the account from which it came was falsely and fraudulently obtained.
27 That messages could not be sent "arbitrarily" is irrelevant (and an

Case
2:07-cv-01929-ABC-AGR

1 inaccurate factual statement as discussed above) -- nothing in this
2 subsection requires that messages must be sent "arbitrarily" and
3 reading such a requirement into the statute would seriously undermine
4 the efficacy of this subsection. Therefore, Plaintiff has
5 demonstrated a likelihood of success on its claim under section
6 7704(a)(1).

7 b. § 7704(a)(3)

8 Section 7704(a)(3) prohibits sending commercial electronic mail
9 that does not contain a functioning return electronic mail address,
10 active for at least 30 days following the date of the message, to
11 which a recipient can send a request that no further messages be sent.
12 15 U.S.C. § 7704(a)(3)(A). To bring a private cause of action under
13 this subsection, Plaintiff must demonstrate a "pattern or practice" of
14 prohibited conduct. Id. § 7706(g)(1). Plaintiff argues that
15 Defendant violated this provision by sending messages from other
16 users' accounts, so that any reply message sent by a user to decline
17 further messages would go to the unwitting sender, not to Defendant.
18 Defendant argues that a recipient can, in fact, reply to a message
19 sent from another user because the messages contain information on the
20 sender and the sender must be on the recipient's "friends" list to
21 send the message in the first place.

22 Defendant again ignores the plain language of the Act. The
23 subsection requires that messages contain a functioning return
24 electronic mail address to which a recipient can respond to request no
25 further messages. Defendant's use of "hijacked" profiles to send
26 messages from a user other than Defendant completely eviscerates a
27 recipient's ability to request no further messages from the actual

1 spammer. Any request to stop sending messages would not go to the
2 individual responsible for the spam message, but rather, to an
3 unwitting sender who cannot control Defendant's surreptitious use of
4 their account. Congress clearly intended this provision to enable
5 recipients of commercial spam to contact the spammer to curb further
6 spamming. Interpreting it as advocated by Defendant would undercut
7 this purpose and encourage "hijacking" as an end-run around this
8 subsection.

9 Plaintiff asserts that Defendant's prohibited conduct under this
10 subsection amounted to a "pattern or practice" of violations and
11 Defendant makes no argument specifically refuting this contention.
12 The terms "pattern or practice" are undefined in the Act, but in other
13 contexts, the Ninth Circuit has stated that "these terms have their
14 ordinary meaning." Cherosky v. Henderson, 330 F.3d 1243, 1246-47 (9th
15 Cir. 2003); see also United States v. Ironworkers Local 86, 443 F.2d
16 544, 552 (9th Cir. 1971) ("The words [pattern or practice] were not
17 intended to be words of art."). One isolated act in violation of the
18 Act is insufficient. See Omega World Travel, Inc. v. Mummagraphics,
19 Inc., 469 F.3d 348, 358 (4th Cir. 2006) (granting summary judgment on
20 section 7704(a)(3) claim because one violation did not demonstrate a
21 pattern or practice). The evidence indicates that, beginning as early
22 as October 2006, Defendant began his activities to obtain MySpace.com
23 members' log-in information and to send out unsolicited emails.
24 (Frazier Decl. ¶¶ 2-3.) Specifically, Plaintiffs offered evidence of
25 at least three separate "attacks" by Defendant using other members'
26 profiles to send commercial messages:

- 27 • On March 27, 2007, Plaintiff's abuse team discovered that

1 Defendant used 328,303 profiles to send 392,726 unsolicited
2 messages. (Id. ¶ 7.)

- 3 • On May 16, 2007, the abuse team discovered that Defendant
4 used at least 5,306 user profiles to send 5,783 unsolicited
5 messages. (Id. ¶ 9.)
- 6 • On May 20, 2007, the abuse team discovered that Defendant
7 used 8,935 user profiles to send at least 10,125 unsolicited
8 messages. (Id. ¶ 8.)
- 9 • Since Plaintiff filed its motion, the abuse team has
10 discovered an additional 110,000 messages sent from 76,200
11 user accounts between May 10, 2007 and June 14, 2007.
12 (Kaleel Supp. Decl. ¶ 11.)

13 This detailed record adequately demonstrates that Defendant has
14 engaged in a pattern of violations sufficient under section 7706(g)(1)
15 to support Plaintiff's private cause of action. Therefore, Plaintiff
16 has demonstrated a likelihood of succeeding on its section 7704(a)(3)
17 claim.

18 c. § 7704(a)(5)

19 Section 7704(a)(5) requires that all commercial electronic
20 messages contain "clear and conspicuous identification that the
21 message is an advertisement or solicitation," "clear and conspicuous
22 notice of the opportunity to decline to receive further commercial
23 electronic mail messages from the sender," and "a valid physical
24 postal address of the sender." 15 U.S.C. § 7704(a)(5)(A). This
25 provision also requires Plaintiff to demonstrate a pattern or practice
26 of violations. Id. § 7706(g)(1).

27 Plaintiff claims that Defendant violated this provision with
28 400,000 messages that did not identify themselves as advertisements,
did not contain notice of an opportunity to opt out of receiving
further messages, and did not contain a physical address for
Defendant. Plaintiff also argues that this information was absent

1 from messages sent from users' hijacked accounts. Defendant argues
2 that the messages were not "commercial," but rather invitations to
3 view pictures, e-cards, or other non-commercial material, and even so,
4 the messages contained a MySpace.com return address.

5 The Act defines "commercial electronic mail message" as "any
6 electronic mail message the primary purpose of which is the commercial
7 advertisement or promotion of a commercial product or service
8 (including content on an Internet website operated for a commercial
9 purpose)." 15 U.S.C. § 7702(2)(A). Regulations passed under the Act
10 further define the term "primary purpose" as "an electronic mail
11 message [that] consists exclusively of the commercial advertisement or
12 promotion of a commercial product or service[.]" 16 C.F.R
13 316.3(a)(1). The plain language of this subsection indicates that
14 "commercial electronic mail messages" include messages that may not
15 themselves appear commercial, but that promote a "commercial service"
16 such as an "Internet website operated for a commercial purpose." 15
17 U.S.C. § 7704(a)(5)(A). Although the Wallace Websites do not appear
18 to request any money directly from visitors and Defendant created the
19 websites to "provide fun, viral websites designed to motivate Internet
20 user[s] to refer their friends to view the content, sometimes called a
21 'tell-a-friend' service," (Wallace Decl. ¶ 3, Exh. C.), Defendant
22 admits that his "Internet business" earns him approximately \$1 million
23 per year (Id. ¶ 15). The record is silent as to how Defendant
24 specifically earns this revenue, but evidence on this point is
25 unnecessary. The Court can readily infer that Defendant operates the
26 Wallace Websites, his "Internet business," to generate his \$1 million
27 a year in revenue, and the facts demonstrate that he sent hundreds of

0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1 thousands of messages directing recipients to these websites.
2 Therefore, these messages, even if not commercial on their face,
3 promote an "Internet website operated for a commercial purpose" and
4 are "commercial electronic mail messages" subject to the Act.

5 Defendant does not dispute that the messages did not contain
6 "clear and conspicuous identification that the message is an
7 advertisement or solicitation," "clear and conspicuous notice of the
8 opportunity to decline to receive further commercial electronic mail
9 messages from the sender," and "a valid physical postal address of the
10 sender." Further, even if the messages Defendant sent from "hijacked"
11 accounts contained a return address, that address would be wholly
12 ineffective to allow the recipient to "opt out" of receiving further
13 messages since Defendant -- the one engaging in the commercial
14 solicitation -- would never receive those requests. Finally, as
15 discussed above, the evidence submitted by Plaintiff demonstrates a
16 pattern of acts that violate this subsection. Therefore, Plaintiff
17 has demonstrated a likelihood of success on the merits of its claim
18 under section 7704(a)(5).

19 d. Section 7704(b)(2)

20 Section 7704(b)(2) prohibits a person from using "scripts or
21 other automated means to register for multiple electronic mail
22 accounts or online user accounts from which to transmit . . . a
23 commercial electronic mail message that is unlawful under subsection
24 (a)" of section 7704. 15 U.S.C. § 7704(b)(2). Showing a pattern or
25 practice under this provision is unnecessary to maintain a private
26 cause of action. Id. § 7706(g)(1). Plaintiff argues that the Court
27 should infer a violation of this section because the naming

1 conventions used in creating 11,000 separate profiles were consistent,
2 including 2,077 profiles named "What Pic Should I Upload?", as were
3 the naming conventions in the underlying America Online email
4 addresses. (Kaleel Decl. ¶¶ 16-18.) Defendant argues that Plaintiff
5 has presented no evidence that he used a "bot" to register these
6 profiles and in any event, each registration requires the user to
7 input a unique set of characters designed to be unreadable to an
8 automated program, and Plaintiff has not offered any evidence on how
9 such an automated script could be written.

10 Plaintiff need not necessarily provide direct evidence that
11 Defendant used an automated bot for registration, but it must provide
12 evidence sufficient for the Court to infer such use, and Plaintiff has
13 failed to do so. Plaintiff's only evidence is the creation of 11,000
14 profiles, 2,000 of which share the same name, and all of which were
15 registered using similar America Online email addresses. These facts
16 do not necessarily compel the conclusion that Defendant used an
17 automated bot. For example, Plaintiff has not provided evidence of
18 the time frame in which the 11,000 profiles were created, which is
19 crucial because, assuming registration of a new profile takes only one
20 minute (which is conservative given that the user must input a name,
21 country, zip code, birth date, gender, an email address, and a unique
22 verification code, as well as create a password and agree to the TOU
23 Contract), one person could spend 23 eight-hour days, without breaks,
24 to create 11,000 profiles. While this may seem unrealistic, Defendant
25 could also have hired others to assist in this registration process,
26 substantially reducing the time and effort needed from a single
27 person. On the other hand, evidence that the registration of the

1 11,000 profiles occurred over a matter of hours or even days would
2 greatly strengthen any inference that the registration was done with
3 an automated bot.

4 Moreover, Plaintiff has provided no evidence that an automated
5 bot could circumvent the verification step in the registration
6 process, a security measure used by Plaintiff to stop automated
7 registration. Plaintiff suggests instead that Defendant could have
8 used an automated bot to complete all steps up to the verification
9 code step. While this may be true, and the Court certainly would not
10 require Plaintiff to disclose trade secrets or outline the specific
11 steps to circumvent its security measures to prove this point, the
12 record is devoid of any testimony that this type of automated bot
13 exists or has been used in the past. Defendant, on the other hand,
14 testified that he has no knowledge of any automated script that could
15 circumvent this security measure. (Wallace Decl. ¶ 9.) The Court
16 recognizes that at the preliminary stage the evidentiary burden is
17 relaxed, see Flynt Distrib. Co. v. Harvey, 734 F.2d 1389, 1394 (9th
18 Cir. 1984), but the evidence in the record at this time is simply
19 insufficient to demonstrate that Plaintiff will likely prevail on the
20 merits of its claim under this subsection.

21 **B. Irreparable Harm**

22 Plaintiff claims it has been irreparably harmed by Defendant's
23 activities because Defendant's messages have clogged the MySpace.com
24 network, used up bandwidth, and degraded the user experience. (Kaleel
25 Decl. ¶¶ 11-12.) This has resulted in delivery-related costs, and
26 costs associated with devoting time, money, and resources to stop
27 Defendant's activities. (Kaleel Decl. ¶ 21.) Moreover, Plaintiff's

SCANNED

1 reputation and business goodwill have suffered, manifested by 800
2 complaints lodged by users over Defendant's activities. (Frazier
3 Decl. ¶ 15.)²

4 Harm to business goodwill and reputation is unquantifiable and
5 considered irreparable. See Rent-A-Center, Inc. v. Canyon Tele. &
6 Appliance Rental, Inc., 944 F.2d 597, 603 (9th Cir. 1991) ("Intangible
7 injuries, such as damage to ongoing recruitment efforts and goodwill,
8 qualify as irreparable harm."); Optinrealbig.com, LLC v. Ironport
9 Sys., Inc., 323 F. Supp. 2d 1037, 1050 (N.D. Cal. 2004) ("Damage to a
10 business's goodwill is typically irreparable injury because it is
11 difficult to calculate."). Plaintiff has incurred substantial costs
12 in detecting, investigating, and remedying Defendant's unsolicited
13 messages, including removing over 290,000 unauthorized links and over
14 890,000 comments throughout the MySpace.com site. (Frazier Decl. ¶¶
15 13-14.) Moreover, Plaintiff has received 800 complaints about
16 Defendant from users. While that may only amount to one complaint for
17 every thousand unsolicited messages, this is still a substantial
18 number and constitutes injury to Plaintiff's goodwill. (Kaleel Supp.
19 Decl. ¶ 8); see Compuserve Inc. v. Cyber Promotions, Inc., 962 F.
20 Supp. 1015, 1023 (S.D. Ohio 1997) (finding that Defendant Wallace
21 inflicted harm to plaintiff's business reputation and goodwill by
22 causing subscribers to terminate their accounts). Further, the Court

23
24 ²Plaintiff also argues that, since users as young as fourteen
25 years old can create profiles on MySpace.com, Defendant's activities
26 create the risk that minors using MySpace.com might view adult
27 material contained on the Wallace Websites. (Frazier Decl. ¶ 8, Exh.
28 G; Kaleel Decl. ¶ 14.) Defendant disputes this contention. The Court
need not address this point since Plaintiff sufficiently demonstrated
irreparable harm through the other evidence it has submitted.

ORIGINAL

1 cannot expect every user to complain about every piece of spam
 2 received, since users would spend as much time responding to spam as
 3 they would responding to non-spam messages. See 15 U.S.C. § 7701(2)
 4 ("Unsolicited commercial electronic mail is currently estimated to
 5 account for over half of all electronic mail traffic . . .").
 6 Moreover, Defendant's misleading suggestions that he is affiliated
 7 with Plaintiff impacts the quality of MySpace.com users' experiences
 8 with Plaintiff's services. See Hotmail Corp. v. Van\$ Money Pie Inc.,
 9 47 U.S.P.Q.2d 1020, 1025-26 (N.D. Cal. 1998) (finding irreparable harm
 10 where defendants caused customer confusion by suggesting they were
 11 associated with plaintiff); Meineke Car Care Centers, Inc. v.
 12 Quinones, 2006 WL 1549708, *3 (W.D.N.C. 2006) (finding that lost
 13 customers resulting from defendants' deceptive suggestion that they
 14 were associated with plaintiff constituted irreparable harm).³ For
 15 these reasons, Plaintiff has persuasively demonstrated irreparable
 16 harm from Defendant's unlawful activities.

C. Balance of Hardships and Public Interest

17
 18 The balance of hardships tips sharply in favor of Plaintiff here.
 19 Plaintiff has already expended substantial time and money in combating
 20 Defendant's unsolicited messages and postings, and has dealt with over
 21 800 resulting user complaints. Moreover, Plaintiff has discovered

22
 23 ³Defendant distinguishes Hotmail Corp. on the ground that it
 24 involved a claim for trademark infringement. Although that is true,
 25 the irreparable harm inquiry is not dependent on the claims asserted,
 26 but rather the harm suffered as a result of the defendant's allegedly
 27 unlawful actions. Here, Defendant caused confusion by using the
 MySpace.com logo and log-in box to deceive users into providing their
 log-in information. This activity creates the same risk of harm as in
Hotmail Corp. -- the potential loss of customers -- and therefore the
 court's analysis in that case is equally applicable here.

1 further evidence that Defendant's actions have continued even after
2 Plaintiff filed the instant motion, discovering yet another group of
3 110,000 messages sent from 76,200 user accounts between May 10, 2007
4 and June 14, 2007. (Kaleel Supp. Decl. ¶ 11.) Plaintiff also
5 suggests that, short of an injunction, it would experience difficulty
6 in curbing Defendant's activities by, for example, blocking
7 Defendant's Internet Protocol addresses, without also curbing other
8 users' legitimate use. (Kaleel Supp. Decl. ¶ 5.) Even if it blocked
9 his IP addresses, he could modify his equipment and tactics to
10 circumvent this security measure. See, e.g., Compuserve Inc., 962 F.
11 Supp. at 1019 (stating that, in response to software programs blocking
12 Defendant Wallace and his company's messages, they "have modified
13 their equipment and the messages they send in such a fashion as to
14 circumvent Compuserve's screening software."). In contrast, as
15 outlined above, Defendant's actions likely violate the CAN-SPAM Act
16 and he would experience no hardship if enjoined from committing any
17 further violations. See Phillip Morris USA Inc. v. Shalabi, 352 F.
18 Supp. 2d 1067, 1075 (C.D. Cal. 2004).

19 The public interest is also served through enjoining Defendant's
20 unlawful activities. In passing the CAN-SPAM Act, Congress recognized
21 the significant costs and burden associated with the nearly unchecked
22 growth of commercial spam. 15 U.S.C. § 7701. "[B]arraging the public
23 with spam" injures the public such that the public "is forced to incur
24 the costs of needlessly expended energy and time evaluating and
25 eventually discarding defendants' unsolicited messages[.]" F.T.C. v.
26 Phoenix Avatar, LLC, 2004 WL 1746698, *14 (N.D. Ill. 2004) (enjoining
27 violations of the CAN-SPAM Act). Because Defendant's activities fall

SCANNED

1 squarely within those activities Congress found detrimental to the
2 public in the CAN-SPAM Act, this factor strongly weighs in favor of
3 Plaintiff.

4 **IV. SCOPE OF INJUNCTION**

5 Defendant challenges Plaintiff's proposed injunction as too
6 broad, sweeping in Defendant's legitimate activities along with any
7 alleged unlawful ones. Plaintiff's proposed injunction seeks to
8 enjoin Defendant from the following:

9 (a) "accessing or using the MySpace.com website, MySpace Internet
10 messaging service and/or any other services offered by or through
11 MySpace (the 'MySpace Service') to directly or indirectly send or
12 transmit any electronic communications, emails or instant
13 messages to any MySpace user or MySpace account or to post
14 comments or bulletins";

15 (b) "establishing or maintaining MySpace profiles or accounts";

16 (c) "using the MySpace Service for a commercial purpose";

17 (d) "referring in any way to MySpace in connection with any
18 unsolicited commercial electronic communication, email or
19 instant message";

20 (e) "using any automated scripts, bots, or other executable
21 programs in connection with any MySpace account or the
22 MySpace service or providing such programs to third parties
23 for use on the MySpace Service";

24 (f) "soliciting, requesting, or taking any action to induce
25 a MySpace user to provide identifying information, including
26 MySpace account information such as a username and/or
27 password"; and

28 (g) "using another MySpace user's identifying information,
including MySpace account information such as username
and/or password";

(h) "referencing MySpace in connection with any
advertisements []"; and

(i) "[encouraging], facilitating, enabling or inducing any
person or entity to do any of the above in violation of the
CAN SPAM Act, 15 U.S.C. § 7701 et seq. and California
Business & Professions Code §§ 17529.5, 17200 et seq., 17500
et seq., and 22948."

1 Defendant argues that subsections (d) and (h) sweep in legitimate
2 commercial speech in violation of his First Amendment rights.
3 Plaintiff refutes this claim by citing two cases to suggest that
4 courts have rejected Defendant's First Amendment arguments in similar
5 circumstances. See Cyber Promotions v. America Online, Inc., 948 F.
6 Supp. 436, 455 n.7 (E.D. Pa. 1996); Compuserve, 962 F. Supp. at 1024.
7 Plaintiff, however, misinterprets the opinions in both America Online
8 and Compuserve. In America Online, the court specifically limited its
9 discussion to activities on the America Online site, not on the
10 Internet, stating that "AOL has never sought to control the exchange
11 of ideas and communications over the Internet itself. Rather, AOL has
12 sought to control its own pathway or channel leading to the Internet
13 in order [to] protect its own private property, reputation and
14 subscribers from Cyber's mass email advertisements." 948 F. Supp. at
15 454-455. Similarly, in Compuserve, the court's analysis centered on
16 "Defendant's use of plaintiff's proprietary computer equipment," not
17 on regulating the channels of speech on the greater Internet. 962 F.
18 Supp. at 1027.

19 The Court finds that subsections (d) and (h) are, in fact, too
20 broad, risking infringement of Defendant's legitimate commercial and
21 non-commercial speech activities outside Plaintiff's proprietary
22 MySpace.com site and beyond the limitations upheld in America Online
23 and Compuserve. Defendant has a legitimate First Amendment right to
24 mention Plaintiff, even in commercial solicitation messages, so long
25 as recipients are not misled into believing that Defendant is somehow
26 associated with or speaking for Plaintiff. For example, Defendant has
27 the right, in any commercial message, to engage in critical discussion

CONFIDENTIAL

1 of Plaintiff, Plaintiff's lawsuit against him, or to truthfully
2 discourage recipients from utilizing Plaintiff's services. As both
3 subsections (d) and (h) are currently drafted, Defendant could not
4 engage in this speech and enjoining Defendant consistent with these
5 provisions would, in fact, violate Defendant's free speech rights.

6 Subsections (f) and (g) also risk curbing the legitimate
7 activities of third parties. As they are drafted, subsections (f) and
8 (g) would preclude Defendant from obtaining fully informed, knowing,
9 and voluntary consent from MySpace.com members so that Defendant might
10 log on to their accounts and disseminate messages (commercial or
11 otherwise). Although the record does not reflect that any member has
12 (or would) consent to such a use of his or her account, this
13 possibility exists and the Court cannot enjoin this legitimate choice
14 by members, so long as Defendant fully informs them that he is not
15 affiliated with or sanctioned by Plaintiff, and that he intends to use
16 that information to log in to their MySpace.com accounts and
17 disseminate messages to other MySpace.com users. Therefore,
18 subsections (f) and (g) are too broad.

19 Further, the Court cannot enjoin Defendant based on subsection
20 (e) because, as discussed above, the Court finds that Plaintiff has
21 not demonstrated a likelihood of success on the merits of its section
22 7704(b)(2) claim. The Court notes that omitting this subsection of
23 the proposed injunction on this basis may have little practical effect
24 since subsection (b) prevents Defendant from establishing MySpace.com
25 accounts or profiles by any means, including through automated bots.

26 The remaining provisions (a), (b), and (c) relate specifically to
27 Defendant's use of Plaintiff's space, equipment, and property. As

1 Plaintiff points out, MySpace.com is a private site, the use of which
2 is a privilege, and Defendant has repeatedly demonstrated his
3 inability to comply with Plaintiff's rules of use or with federal law
4 when using Plaintiff's services. Therefore, these provisions validly
5 prevent Defendant from abusing the privilege of using Plaintiff's
6 services and are adequate in scope to fulfill this purpose.⁴

7 **V. BOND**

8 Federal Rule of Civil Procedure 65(c) requires Plaintiff to post
9 a bond, in a sum the Court deems appropriate, for the payment of costs
10 and damages that Defendant may suffer if he is later found to have
11 been wrongfully enjoined. While the Court recognizes that a bond may
12 not be required when the harm to the enjoined party is minimal, see,
13 e.g., Jorgensen v. Cassidy, 320 F.3d 906, 919 (9th Cir. 2003), the
14 Court retains discretion to require a bond when the party seeking the
15 injunction has not offered evidence of its own harm in posting a bond,
16 see Barahona-Gomez v. Reno, 167 F.3d 1228, 1237 (9th Cir. 1999).

17 Plaintiff has argued only that an injunction would impose no hardship
18 on Defendant, not that Plaintiff itself will suffer some harm in
19 posting a bond. Plaintiff requests a bond of \$1 million, but the
20 Court finds that a bond for this amount is unnecessary. Therefore,
21 the Court ORDERS Plaintiff to post a bond in the amount of \$50,000.

22 **VI. CONCLUSION**

23 Plaintiff has demonstrated a likelihood of success on the merits

24
25 ⁴The Court notes that subsection (i) is necessary to the extent
26 that it enjoins Defendant from directing others to undertake
27 activities that he is prohibited from undertaking, although referring
to the specific statutory provisions at issue is unnecessary because
the other parts of the injunction clearly delineate the prohibited
conduct.

1 of its claims under the CAN-SPAM Act, 15 U.S.C. § 7704(a)(1), (a)(3),
2 and (a)(5), but has not offered sufficient evidence to demonstrate a
3 violation of section 7704(b)(2). Plaintiff has also demonstrated
4 irreparable harm to its business goodwill and reputation if Defendant
5 continues his unlawful activities, the balance of hardships tips in
6 its favor, and the public interest is served by enjoining Defendant's
7 conduct.

8 Therefore, the Court ENJOINS Defendant, his agents, servants,
9 employees, representatives, and all other persons or entities acting
10 on his behalf or in concert or participation with him, from⁵:

11 (1) accessing or using the MySpace.com website, MySpace Internet
12 messaging service and/or any other services offered by or through
13 MySpace (the 'MySpace Service') to directly or indirectly send or
14 transmit any electronic communications, emails or instant
15 messages to any MySpace user or MySpace account or to post
16 comments or bulletins;

17 (2) establishing or maintaining MySpace profiles or accounts;

18 (3) using the MySpace Service for a commercial purpose;

19 (4) referring to MySpace in connection with any unsolicited
20 commercial electronic communication, email or instant
21 message, in any way that falsely or fraudulently suggests
22 that such message was approved by, generated by, or is in
23 any way affiliated with MySpace;

24 (5) using any MySpace logo or using any graphic, interface,
25 or other presentation that approximates or resembles the
26 MySpace.com log-in page to mislead users into believing that
27 they are logging onto their MySpace.com accounts rather than
28 providing Defendant with their username and password;

(6) inducing a MySpace user to provide MySpace identifying
information, including MySpace account information such as a
username and/or password, without first informing the user
the Defendant is not affiliated with or sanctioned by
MySpace and without obtaining fully informed, knowing, and
voluntary consent through a separate affirmative step by the

⁵These provisions incorporate a combination of Plaintiff's proposed provisions and the Court's limitations as outlined supra.

SCANNED

1 user; and

2 (7) encouraging, facilitating, enabling or inducing any
3 person or entity to do any of the above.

4 Plaintiff is ORDERED to post a bond in the amount of \$50,000
5 within ten (10) days of the date of this Order. Plaintiff is also
6 ORDERED to prepare a proposed order consistent with this Order,
7 including findings of fact and conclusions of law, within ten (10)
8 days of the date of this Order.

9 IT IS SO ORDERED.

10 DATED:

July 2, 2007

Audrey B. Collins

AUDREY B. COLLINS
UNITED STATES DISTRICT JUDGE