MITCHELL | HAMLINE School of Law

William Mitchell Law Review

Volume 27 | Issue 3 Article 19

2001

Spam Remedies

Dianne Plunkett Latham

SPAM REMEDIES

Dianne Plunkett Latham†

I. INTRODUCTION

Spam, or unwanted electronic mail, has bogged down the Internet and sometimes even brought it to a halt in denial-of-service attacks. Spam spewers have perpetrated fraud and other crimes. The purpose of this article is to discuss spam remedies such as litigation and its associated case law, state and federal legislation, the Attorney General's response, as well as techniques for tracking down the source of spam.

Nearly everyone with an e-mail address has received unwanted electronic solicitations, or spam.[1] "Junk e-mail" accounts for much

† Member Minnesota Bar. Ms. Plunkett Latham received her B.A. from the University of Illinois in Urbana in 1968 and her J.D. from William Mitchell College of Law in 1986 where she was Executive Editor of the William Mitchell Law Review. Ms. Plunkett Latham is a patent attorney in Edina, Minnesota. She is the past President of the Minnesota Intellectual Property Law Association, as well as the past Chair of the Minnesota State Bar Association Computer Law Section. She is currently the editor of the Minnesota State Bar Association Computer Law Section Computer Law News.

1. .SPAM® (Spiced Pork And Ham) in upper case letters is the registered

of all incoming mail on the Internet. Internet Service Providers (ISP's) and individuals often respond to spam by blacklisting,[2] or filtering out the domain names that are the apparent source of the spam. Likewise, many network administrators have started to filter out all connections from known "spamhaus" operations.

To combat this rejection, spammers conceal their identity through illegal practices known as "forged spamming" (or "spoofing") as well as "domain name hijacking." "Forged spamming" occurs when spammers broadcast from bulk-friendly domains using false domain names. Spammers choose a prestigious domain name believing that their mail will be accorded more attention.

"Hijacking" occurs when massive amounts of mail are relayed through an unsuspecting server. Spammers typically send their unwanted solicitations through the "hijacked" server during off-peak hours when operations are at lower staffing levels and less likely to attract notice. Spammers search for open relays in another's mail server and "hijack" the server in a practice called "domain name hijacking." When a message is relayed, it is first sent to a host that delivers it to the final recipient. This practice permits the spam to originate (admittedly involuntarily) from the hijacked server, giving it unwarranted credibility. The spammers, in effect, launder their junk e-mail through third-party relays to enable them to slip through the spam filters.

Spammers also use relays to increase the number of messages they can spew. A PC on the end of a phone line can only pump out a limited number of messages. Hijacking a high-powered mail host with a high-speed connection, allows them to push through hundreds of times more junk mail. Relaying through several mail servers in parallel, permits a flood of extraordinary amounts of junk e-mail.[3]

The unauthorized use of another's domain name as a spammer's return address, results in responses which clog up the legiti-

---

trademark of Hormel Foods. Spam in lower case letters is the term associated with junk e-mail. The term spam is not an acronym, but rather is named after the Spam Sketch #25 from the second series of "Monte Python's Flying Circus" recorded June 25, 1970 and aired on television on December 15, 1970. *See generally* www.acns.fsu.edu/special/features/no4/python (last visited Nov. 17, 2000) (repeating and singing spam menu entries in a restaurant setting ad-nausea).

2. For a blacklist used by many organizations on the net, go to the Mail Abuse Prevention System Realtime Blackhole List, *at* http://www.maps.vix.com/rbl/ (last visited Oct. 25, 2000).

3. Chip Rosenthal, What is Third-Party Mail Relay?, *at* http://mail-abuse.org/tsi/ar-what.html (last modified July 31, 1999).

mate network with the returned e-mail from inactive accounts, as well as clogging the legitimate network with flames (irate recipient's messages). A major spam attack can bog down or crash a server in a denial-of-service attack, resulting in the loss of a company's time and money.

II. CASE LAW

The list of potential offenses spammers commit is extensive and includes false designation of origin[4] and dilution of interest in service marks[5] under the Lanham Act, state and common law unfair competition, exceeding authorized access and impairing computer facilities in violation of the Computer Fraud and Abuse Act,[6] violation of state computer crimes acts, deceptive trade practices,[7] defamation, fraud,[8] forgery, harassment, theft, libel, breach of contract, false statements in advertising,[9] and common law trespass to chattels. Tracking down spammers in cyberspace is more difficult than finding legal theories under which to charge them. Enjoining those who send spam has generally been successful[10]—provided you can identify the source. Recovering damages from those who hire spam houses as independent contractors to send spam for them, however, has been less successful.[11]

A. America Online, Inc. v. LCGM, Inc.

ISP's such as America Online, Inc. (AOL) and Hotmail have aggressively sought injunctions and damages against spammers. In *America Online, Inc. v. LCGM, Inc.*,[12] the defendants admitted maintaining AOL memberships to collect e-mail addresses of other AOL members through AOL chat rooms. The defendants then forged

4. 15 U.S.C. § 1125(a)(1) (1994 & Supp. 1998).
5. *Id.* § 1125(c)(1).
6. 18 U.S.C. § 1030 (1994 & Supp. 1998).
7. MINN. STAT. § 325D.43-48 (West 1995 & Supp. 2000).
8. *Id.* § 325F.68-69.
9. *Id.* § 325F.67.
10. *E.g.*, Classified Ventures, L.L.C. v. Softcell Mktg., Inc., 109 F. Supp. 2d 898 (N.D. Ill. 2000); America Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444 (E.D. Va. 1998); Hotmail Corp. v. Van$ Money Pie, Inc., 47 U.S.P.Q.2d (BNA) 1020 (N.D. Cal. 1998); America Online, Inc. v. IMS, 24 F. Supp. 2d 548 (E.D. Va. 1998); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997).
11. *See generally* Seidl v. Greentree Mortgage Co., 30 F. Supp. 2d 1292 (D. Colo. 1998).
12. *America Online*, 46 F. Supp. 2d at 444.

the domain information "aol.com" in the "from" line of the e-mail messages sent to AOL members and caused the AOL domain name to appear in the electronic header information of their commercial e-mails. The defendants sent e-mail messages from their computers through their network via e-mail software to AOL, which then relayed the messages to AOL members. As a result, many AOL members expressed confusion about whether AOL endorsed the defendants' pornographic web sites or their bulk e-mailing practices.[13] The court granted AOL's Motion for Summary Judgment with respect to its claims of false designation of origin and dilution of interest in service marks under the Lanham Act, as well as exceeding authorized access and impairing computer facilities in violation of the Computer Fraud and Abuse Act, violation of the Virginia Computer Crimes Act, and trespass to chattels under the Common Law of Virginia.[14]

B. Hotmail Corp. v. Van$ Money Pie, Inc.

The Northern District of California in *Hotmail Corp. v. Van$ Money Pie, Inc.*[15] temporarily and preliminarily enjoined the defendants from sending electronic mail bearing false or invalid return information or containing the domain name "hotmail.com."[16] Hotmail provides free electronic mail for over ten million subscribers.[17] The Hotmail subscriber Service Agreement specifically prohibits subscribers from using Hotmail to send unsolicited bulk e-mail and permits Hotmail to terminate accounts of subscribers who violate the terms of service. The defendants established Hotmail accounts for the purpose of collecting responses to their e-mails. The defendants returned invalidly addressed messages for what was in effect a "drop box," whose contents were never read.[18] The defendants falsely designated an actual Hotmail e-mail address as the point of origin.[19] Hotmail's successful legal claims included false designation of origin, federal and state dilution, violation of the Computer Fraud and Abuse Act, state and common law unfair competition, breach of contract, fraud and misrepresentation, and

13. *Id.* at 448.
14. *Id.* at 446.
15. *Hotmail Corp.*, 47 U.S.P.Q.2d (BNA) 1020 (N.D. Cal. 1998).
16. *Id.* at 1026.
17. *Id.* at 1021.
18. *Id.*
19. *Id.* at 1022.

trespass to chattels.[20]

C. Seidl v. Greentree Mortgage Co.

The plaintiff in *Seidl v. Greentree Mortgage Co.*[21] was not as successful as were the previous plaintiffs, AOL and Hotmail. The defendant, Greentree Mortgage Company, hired Mark Van Keuren, a sole proprietor conducting business under the name Modern Computing, on a one-time, flat fee basis to advertise its mortgages using a bulk e-mail advertising campaign to a set number of e-mail users. Greentree provided the body of the advertisement, which contained Greentree's 800-telephone number and its e-mail address, mfgtm@aol.com. The time and manner of sending the e-mail as well as the choice of recipients was up to Van Keuren, who used his own equipment and his own mailing list.[22] Van Keuren chose to use the e-mail address nobody@localhost.com in both the "From" and "Reply to" and configured the e-mail headers to include them. As a result, e-mails with invalid addresses bounced back to localhost.com, as did the replies.[23] Seidl, who owned the domain name localhost.com, did not have a "nobody" designation, but the e-mail came to him anyway because of his domain name, localhost.com.[24]

In 1995, Mr. Seidl, a graduate student in computer science at Colorado University, registered the domain name nobody@localhost.com with Network Solutions, Inc., for Wraith Interprises (sic), an entity that he had not used.[25] Seidl testified that he registered "nobody@localhost.com" as a gag or to keep a telemarketer from getting the name. His computer received over 7,000 bounce backs from the Greentree e-mail advertisement and he was unable to use his computer for three days. Siedl claimed his reputation among the Internet community suffered.[26] Seidl based his claims on the Colorado Deceptive Trade Practices Act, trespass to chattel and various theories of negligence.[27] Greentree moved for summary judgment on all of plaintiff Siedl's claims, because Van Keuren was an independent contractor and Greentree was not

20. *Id.*
21. *Seidl*, 30 F. Supp. 2d 1292 (D. Colo. 1998).
22. *Id.* at 1297.
23. *Id.*
24. *Id.* at 1297-98.
25. *Id.*
26. *Id.* at 1298.
27. *Id.*

liable for the acts of an independent contractor under Colorado law.[28] The court found Van Keuren to be an independent contractor precluding Greentree from vicarious liability.[29]

The court reasoned that

> Greentree took advantage of an available, legal, but controversial vehicle for advertising its business by hiring someone to send unsolicited advertisements by e-mail, with unintended consequences to Mr. Seidl. Mr. Seidl, a private citizen with an ax to grind about the political/social issue of spamming, transformed the public debate over this issue into a legal dispute with Greentree, an admitted spammer. The lawsuit was for the purpose of publicizing adverse consequences to companies that engaged in spamming. Mr. Seidl and his lawyer, Ms. Sostre attempted, unsuccessfully, to develop a legal theory under which an advertiser could be made to suffer financially for the practice of spamming. It appears to this court that such efforts at changing the law regarding spamming would be more effectively addressed in the legislative arena.[30]

If this same reasoning is followed, companies can insulate themselves from the legal consequences of spamming by hiring a third party independent contractor. Plaintiffs may be left with little recourse for damages from lightly capitalized independent contractors, who are more likely to be judgment-proof, then the companies on whose behalf they spew spam.

D. Individual Investor Group, Inc. v. Howard

The case of *Individual Investor Group, Inc. v. Howard*[31] is one of the first actions commenced under Nevada's Electronic Mail Statute.[32] The Individual Investor Group operates and publishes the *Individual Investor* magazine as well as other Internet and print publications that collectively reach more than 2,000,000 investors and financial professionals monthly. Howard's spam contained Individual Investor Group's trademarks and Internet domain names, thus giving the impression it had come from the Individual Investor

28. *Id.* at 1300.
29. *Id.* at 1301.
30. *Id.* at 1318-19.
31. Individual Investor Group v. Howard, No. CV-S-99-00437-DWH (D. Nev. 1999).
32. NEV. REV. STAT. §§ 41.705–41.735 (2000).

Group. It also contained an inaccurate return address designed to appear as if it was sent from a foreign country, to discourage efforts to track down the spammer.[33]

Using the Internet Protocol (IP) address information in the spam header, Individual Investor Group was able to consult public databases and identify the entity that provided the spammer with ultimate access to the Internet. Originally, the Individual Investor Group action was brought against an unnamed 'John Doe' defendant. Using a Federal subpoena, however, the message ID was traced to the source of the unsolicited e-mails. In January 2000, a settlement was obtained including a permanent injunction, a $5,000 payment, a public apology, and an agreement to assist the Individual Investor Group with clearing its name from various spam blacklists.[34]

III. TRACING THE SOURCE OF SPAM

Legal theories with which to enjoin spammers are plentiful, though identifying the source of the spam is more difficult. Action against spammers must be taken quickly as the electronic trail may be overwritten in the continuing massive e-mail stream. The more experienced spam generators routinely use dummy return addresses to bounce replies. Their real address, however, may be somewhere within the body of the message or better yet, in the spam header.[35]

To trace the source of spam, whether for the purposes of sending a complaint to an ISP's abuse handler[36] in an effort to have the

33. *See generally* Press Release, Individual Investor Group, Inc., *Individual Investor Group, Inc. Obtains Injunction And Public Apology From Sender Of 'Spam' E-Mail That Infringed Trademark*, www.indi.com/prel-010700.htm (Jan. 7, 2000); and Press Release, *Brown Raysman Millstein Felder & Steiner LLP, Brown Raysman Millstein Felder & Steiner LLP Obtains An Injunction And Public Apology In Internet 'Spamming' Lawsuit*, www.brownraysman.com (Jan. 7, 2000).

34. Individual Investor Group v. Howard, No. CV-S-99-00437-DWH (D. Nev. 1999); Press Releases, supra note 33.

35. Steven William Rimmer, *Death to Spam: A Guide to Dealing with Unwanted E-Mail: Commercial Spams*, at http://www.mindworkshop.com/alchemy/nospam.html (1999).

36. Many of the larger Internet Service Providers have created accounts called "Abuse" to receive mail specifically dealing with abuses of the net by their users. To address mail to such accounts, the general format is "abuse@ISP.com." For example, MSN's abuse handler is abuse@MSN.com. Forward the original unsolicited message to the domain's abuse handler, including its entire header. Legitimate ISP's usually will terminate the spammer's account when informed of their activities.

spammer's e-mail access terminated, or to file litigation, follow this procedure. First, display the message header and find the message ID. The spam e-mail header is less likely to have been altered than the "From" address. Next, take the domain name of the server from which the message was sent, and consult the Network Solutions Inc. (NSI) registry to locate the owner of the originating domain. The Message ID in the header can be used to identify the specific sender.

For example, for Outlook 2000, open the e-mail message. Under the View menu, select Options, and the Internet Headers window will be displayed. If you do not know how to cause your e-mail reader to display an e-mail Header, you can find specific instructions for the major e-mail readers at http://spamcop.net/fomserve/cache/19.html.[37]

Once the Internet header has been opened, find the domain name of the server from which the message was sent. The domain name is the .com (or .net, or .edu, etc.) plus the previous level name, for example, "anywhere.com." The domain name's counterpart IP address consists of four groups of numbers, which define where the server is on the Internet, for example 207.46.181.47. Once you have the domain name you can locate the domain owner using the NSI "Who Is" search engine found at http://www.networksolutions.com/cgi-bin/whois/whois. If the NSI search engine does not find a listing for what appears to be a valid domain name, it is probably bogus. If the domain name is valid, find the Message ID in the header to pinpoint the sender of the offending message. As the message ID is only a string of letters and digits, you may need a court order to cause the originating domain owner to unmask the sender.

If the ISP originating the spam is a bulk-friendly site specializing in spam, confronting the operator of the site will probably be to no avail. Instead, you may need to complain to the originating domain's up-stream provider. You can find out who the up-stream provider is by using the TraceRoute feature that is on-line at: http://cities.lk.net/traceroute.htm. This feature traces the route from your server to the server you have specified, displaying all the "hops" along the way to a maximum of 30 hops. The last hop will be the domain and the IP address of the source of the spam you received. The next to the last hop is the up-stream provider. Unlike the return address, a spam generator cannot falsify the Internet

37. Rimmer, *supra* note 35.

message route.[38]

IV. LEGISLATIVE EFFORTS TO STOP SPAM

A. *State Legislation*

Many states are passing new laws and refining existing laws to better deal with spam. In 1997, Nevada became the first state to pass spam legislation. It was Nevada's Electronic Mail Statute[39] of which the Individual Investor Group availed themselves. At least seventeen additional states have passed spam legislation. These are, California,[40] Colorado,[41] Connecticut,[42] Delaware,[43] Idaho,[44] Illinois,[45] Iowa,[46] Louisiana,[47] Missouri,[48] North Carolina,[49] Oklahoma,[50] Pennsylvania,[51] Rhode Island,[52] Tennessee,[53] Virginia,[54] Washington State[55] and West Virginia.[56] Other states have pending spam legislation.[57] Most state legislation has penalties for falsely identifying the sender. State legislation, however, varies widely; what is urgently needed is Federal legislation similar to that applicable to "junk faxes"[58] or an amendment to the "junk fax" law so that it includes electronic mail as well. Internet users also need some form of digital Caller ID so that the sender's names cannot be falsified.

---

38. *Id.*
39. NEV. REV. STAT. §§ 41.705–41.735 (Supp. 1999).
40. CAL. BUS. & PROF. CODE §§ 17538.4 & .45 (West 1997 & Supp. 2000).
41. COLO. REV. STAT. § 6-2.5 (West 2000).
42. 1999 CONN. ACTS 99-160 (Reg. Sess.).
43. DEL. CODE ANN. TIT. 11, §§ 931, 937 & 938 (1995 & Supp. 1998) (amended 1999).
44. IDAHO CODE § 48–603E (Michie Supp. 2000).
45. 815 ILL. COMP. STAT. §§ 511/1-15 (West Supp. 2000).
46. IOWA CODE § 714E.1-2 (Supp. 2000).
47. LA. REV. STAT. ANN. §§ 14.73.1 & 14.73.6 (West 2000).
48. MO. ANN. STAT. §§ 407.1300–407.1340 (West 2000).
49. N. C. GEN. STAT. §§ 1-75.4, 14-453, 14-548 & 1.5392A (1999).
50. OKLA. STAT. TIT. 15 § 776.1-4 (1993 & Supp. 2000).
51. 18 PA. CONS. STAT. § 5903 (West Ann. 1983 & Supp. 2000).
52. R. I. GEN. LAWS §§ 11-52-1 & 6-47-2 (1994 & Supp. 1999).
53. TENN. CODE ANN. § 47-18-2501 (Supp. 1999).
54. VA. CODE ANN. §§ 8.01-328.1B, 18.2-152.2, 18.2-152.4, & 18.2-152.12 (Michie 1999).
55. WASH. REV. CODE §§ 19.190.010-.050 (1999).
56. W. VA. CODE ANN. §§ 46A–6G-1 to 46A-6G-5 (Michie 2000).
57. David E. Sorkin, *Spam Laws: United States: State Laws*, at http://www.spamlaws.com/state/index.html (last modified Sept. 19, 2000).
58. 47 U.S.C.A. §§ 227(a)(2), (b)(1)(C), (d)(1)-(2) & e(1)(A) (West Supp. 2000).

B. *Federal Legislation*

At least ten bills are currently pending in the U.S. House of Representatives and U.S. Senate relating to spam, though nothing yet has been enacted.[59] These bills are the Can Spam Act,[60] E-Mail User Protection Act,[61] Inbox Privacy Act of 1999,[62] Internet Freedom Act,[63] Internet Growth and Development Act of 1999,[64] Netizens Protection Act of 1999,[65] Protection Against Scams on Seniors Act of 1999,[66] Telemarketing Fraud and Seniors Protection Act,[67] Unsolicited Electronic Mail Act of 1999,[68] and Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2000.[69] Congressional inaction may be due to a wait and see attitude in favor of self-regulation by the direct marketers and for the Federal Trade Commission to announce regulations dealing with spam.[70]

Legislative efforts have attempted to balance freedom of speech with Opt-in/Opt-out provisions. Opt-out provisions, for example, permit users to forgo receiving spam. ISP's, however, generally oppose such provisions and their burdensome administration, preferring instead a complete ban of spam. ISP's argue that a spammer's freedom of speech does not include the right to force someone to pay to read it. Spammers do not pay for the network resources they use; instead, recipients pay for the resources through their monthly access fees.

As legislation in the United States limiting spam increases, spammers have increasingly used offshore servers to originate their messages. Little legislation dealing with spam currently exists in foreign countries.[71]

---

59. David E. Sorkin, *Spam Laws: United States: Federal Laws*, at http://www.spamlaws.com/federal/index.html (last modified Sept. 19, 2000).
60. H.R. 2162, 106th Cong. (1999).
61. H.R. 1910, 106th Cong. (1999).
62. S. 759, 106th Cong. (1999).
63. H.R. 1686, 106th Cong. (1999).
64. H.R. 1685, 106th Cong. (1999).
65. H.R. 3024, 106th Cong. (1999).
66. H.R. 612, 106th Cong. (1999).
67. S. 699, 106th Cong. (1999).
68. H.R. 3113, 106th Cong. (2000).
69. S. 2542, 106th Cong. (2000).
70. David H. Bernstein, *New Developments In Protecting Intellectual Property Online*, 623 PLI/Proc. 87 (2000).
71. *E.g.*, David E. Serkin, Spam Laws: Other Countries, Spam Laws, *at* http://www.spamlaws.com/world.html (last modified Sept. 19, 2000) (providing information on what foreign countries are doing about spam and other internet abuses).

V. ATTORNEY GENERAL

Private law suits have characterized efforts to attack spam to date. The Minnesota Attorney General's office has taken a hands-off approach. When Minnesota's Attorney General Mike Hatch was asked about the spam issue at the October 19, 1999 MSBA Computer Law Section Annual CLE, he responded,

> It's not one I would put in the top ten ... compared to prostitution, gambling ... We're not going to get money damages ....We can get an injunction .... So what—They'd set up another web site .... It would be interesting if some enterprising person would want to take a class action on that.[72]

Attorney General Hatch added that his problem with addressing spam was one of insufficient resources, "If you give me enough people, I'll go do it."[73] The Attorney General Offices around the country are likely similarly situated.

VI. CONCLUSION

The list of potential offenses spammers commit is extensive. Enjoining those who send spam has generally been successful provided you can identify the source. At least eighteen states have passed spam legislation. Unfortunately, state legislation varies widely. What is urgently needed is federal legislation similar to the "Junk Fax Law" [74] so that it covers electronic mail as well. Internet users need some form of digital caller ID so that sender's names cannot be falsified. At least ten bills are currently pending in the United States Congress. Stronger federal legislation will help reduce the fraud and damages caused by spammers.

72. Mike Hatch, Consumer Fraud in the Cyber Age: Efforts to Protect Minnesotans Against Fraudulent Activities and Internet Crime, 1999 Minnesota State Bar Ass'n Computer Law Institute (MSBA 1999).

73. *Id.*

74. 47 U.S.C.A. §§ 227(a)(2), (b)(1)(C), (d)(1)-(2) & e(1)(A)(West Supp. 2000).

***