Canned Spam: New State and Federal Legislation Attempts to Put a Lid On It

by
Jordan M. Blanke *

I. INTRODUCTION

A. "Have you got anything without spam?"[1]

It has become almost impossible to avoid spam. According to a recent *New York Times* article, of the 3 million e-mail messages that Indiana University receives each day, 45 percent are spam, or unsolicited commercial e-mail.[2] Experts estimate that spam cost American businesses anywhere from $10 billion to $87 billion in 2003.[3] Even when companies invest in filtering software, employees still waste time sifting through the more evasive spam.[4] America Online (AOL), one of the companies most affected by spam and most vigorous in its efforts to fight it, discards approximately 80 percent of the 2.5 billion e-mail messages sent daily to its subscribers.[5] The Federal Trade Commission reported to a Senate committee that AOL "recently blocked an astonishing 2.37 billion pieces of spam in a single day."[6]

Spammers have become extremely aggressive and efficient in collecting e-mail addresses. The FTC reported in its "Spam Harvest" study that 100 percent of e-mail addresses posted in chat rooms, 86 percent of addresses posted in newsgroups and Web pages, and 50 percent of addresses posted in free, personal Web page services have received spam.[7] Also, spam messages often contain false or misleading information. In its "False Claims in Spam" study, the FTC examined a random sampling of 1,000 e-mail messages it had collected.[8] The study found that 20 percent of the messages offered a variety of business investment opportunities, 18 percent offered "adult-oriented products or services," and 17 percent involved financial products, such as

---

* Professor of Computer Information Systems and Law, Stetson School of Business and Economics, Mercer University, Atlanta, Georgia.

1. GRAHAM CHAPMAN ET AL., THE COMPLETE MONTY PYTHON'S FLYING CIRCUS: ALL THE WORDS 27 (Pantheon Books 1989).

2. Saul Hansell, *Totaling Up the Bill for Spam: Wasted Time, Computer and Human, Is Only Part of the Cost*, N.Y. TIMES, July 28, 2003, at C1.

3. *Id.* at C4.

4. *Id.*

5. *Id.*

6. *Prepared Statement of the Federal Trade Commission on "Unsolicited Commercial Email" Before the S. Comm. on Commerce, Sci. & Transp.* 108th Cong. 13 (May 21, 2003) [hereinafter *Prepared Statement*].

7. *Id.* at 6.

8. *Id.* at 7.

credit cards, mortgages, or insurance.[9] It also found that 40 percent of all the spam contained false information in the body of the message (including 90 percent of the business investment opportunities category), 33 percent contained false or misleading information in the "from" line of the message, and 22 percent in the "subject" line (including over one-third of the adult-oriented category).[10] In total, 66 percent of all the spam contained at least one form of deception.[11] The FTC also investigated whether "remove me" or "unsubscribe" options contained in some spam actually worked.[12] It found that 63 percent of the 200 removal links it tested failed to function.[13]

B. "I don't want ANY spam!"[14]

Thirty-six states have enacted statutes that deal with spam in a variety of ways.[15] Table 1 of this article summarizes the spam-related statutes that have

9. *Id*. at 8.

10. *Id*. at 8-9.

11. *Id*. at 9.

12. *Id*. at 6.

13. *Id*.

14. CHAPMAN, *supra* note 1, at 27.

15. *See* ALASKA STAT. § 45.50.479 (Michie Supp. 2003); ARIZ. REV. STAT. §§ 44-1372 to -1372.05 (Supp. 2003); ARK. CODE ANN. §§ 4-88-601 to -607, 5-41-201 to -205 (Michie 2003); CAL. BUS. & PROF. CODE §§ 17529 to 17529.9, 17538-.45 (West Supp. 2003); CAL. PENAL CODE § 502 (West 1999); COLO. REV. STAT. ANN. §§ 6-2.5-101 to -105 (West 2002); CONN. GEN. STAT. §§ 53-451 to -453 (2003); DEL. CODE ANN. tit. 11, §§ 931, 937, 938 (2001); IDAHO CODE § 48-603E (2003); 815 ILL. COMP. STAT. ANN. 511/1, 5 ,10, 15 (West Supp. 2003); 720 ILL. COMP. STAT. ANN. 5/16D-1 to -3 (West 2003); IND. CODE ANN. §§ 24-5-22-1 to -10 (Michie Supp. 2003); IOWA CODE ANN. § 714E (West 2003); KAN. STAT. ANN. § 50-6,107 (Supp. 2002); LA. REV. STAT. ANN. § 14:73.1, .6 (West Supp. 2003); ME. REV. STAT. ANN. tit. 10, § 1497 (West Supp. 2003); MD. CODE ANN., COM LAW II §§ 14-3001 to –3003 (Supp. 2002); MICH. COMP. LAWS § 445.2501-.2508 (2003); MINN. STAT. ANN. 325F.694 (West Supp. 2004); MO. ANN. STAT. §§ 407.1120-.1147 (West Supp. 2004); NEV. REV. STAT. ANN. 41.705 to .735, 205.492, 205.511, 205.513 (Michie 2002); N.M. STAT. ANN. §§ 57-12-23 to -24 (Michie 2003); N.C. GEN. STAT. §§ 1-75.4, 1-539.2A, 14-453, 14-458 (2003); N.D. CENT. CODE §§ 51-27-01 to 51-27-09 (2003); OHIO REV. CODE ANN. § 2307.64 (Anderson Supp. 2003); OKLA. STAT. ANN. tit. 15, §§ 776.1-.7 (West 2004); 2003 Ore. S.B. 910; 18 PA. CONS. STAT. ANN. §§ 5903, 7661 (West Supp. 2003); 73 PA. CONS. STAT. ANN. § 2250 (West Supp. 2003); R.I. GEN. LAWS §§ 6-47-2, 11-52-1 (2002); S.D. CODIFIED LAWS §§ 37-24-6, -36 to -40 (Michie 2003); TENN. CODE ANN. §§ 47-18-2501 to -2502 (Supp. 2003); TEX. BUS. & COM. CODE ANN. §§ 46.001-.011 (Vernon Supp. 2004); UTAH CODE ANN. §§ 13-36-101 to -105 (Supp. 2003); VA. CODE ANN. §§ 8.01-328.1, 18.2-152.2, 18.2-152.3:1, 18.2-152.4, 18.2-152.12 (Michie Supp. 2003); WASH. REV. CODE ANN.

been enacted in these states. Congress considered several bills before finally enacting one of them. This article examines both the existing state legislation and the proposed and passed federal legislation.

II. State Legislation

A. Definitions

Most states have definitions for some or all of the following: "electronic mail message" (e-mail) or "advertisement," "commercial" or "commercial e-mail," "unsolicited" or "unsolicited commercial e-mail," or "bulk electronic e-mail."[16] Delaware defines both "e-mail" and "commercial e-mail," while Indiana only defines "commercial e-mail"—however, neither defines "unsolicited bulk commercial e-mail" or "unsolicited commercial e-mail."[17] Iowa defines "e-mail," but uses both "bulk e-mail" and "unsolicited e-mail" without further definition.[18] Connecticut, Rhode Island, Tennessee and Virginia all refer to "unsolicited bulk e-mail" without defining any of the individual terms.[19]

Most states define a "commercial e-mail" message as one that advertises or promotes the sale or lease of goods, services, or real property. In the majority of states that define "unsolicited" or "unsolicited commercial e-mail," the key aspects of the definition are the absence of a preexisting personal or professional relationship between sender and recipient and the absence of permission or consent of the recipient. In Louisiana, "unsolicited bulk e-mail" refers only to a message sent "in the same or substantially similar form to more than one thousand recipients."[20] Maine defines an "unsolicited commercial e-mail" as an unrequested e-mail sent to two or more recipients in the state who have no existing business relationship with the sender for the purpose of soliciting charitable contributions or offering goods, services, real property, or information on credit.[21] Some states, partic-

§§ 19.190.010-.050 (West Supp. 2003) ; W. Va. Code §§ 46A-6G-1 to -5 (2003); Wis. Stat. Ann. § 944.25 (West Supp. 2003); Wyo. Stat. Ann. §§ 40-12-401 to -404 (Michie 2002); *see also* David E. Sorkin, *Spam Laws: United States: State Laws at* http://www.spamlaws.com/state/index.html (listing spam-related statutes from thirty-five states) (last visited Feb. 8, 2004).

16. *See infra* app. 1.

17. Del. Code Ann. tit. 11, §§ 931, 937 (2001); Ind. Code Ann. §§ 24-5-22-1 to -10 (Michie Supp. 2003).

18. Iowa Code Ann. § 714E.1 (West 2003).

19. Conn. Gen. Stat. §§ 53-451 to 452 (2003); R.I. Gen. Laws §§ 11-52-1, -4.1 (2002); Tenn. Code Ann. §§ 47-18-2501 to -2502 (Supp. 2003); Va. Code Ann. §§ 18.2-152.2, 18.2-152.3:1, 18.2-152.4, 18.2-152.12 (Michie Supp. 2003).

20. La. Rev. Stat. Ann. §§ 73.1(13) (West Supp. 2004).

21. Me. Rev. Stat. Ann. tit. 10, § 1497(1)(C) (West Supp. 2003).

ularly those that require labeling of adult-oriented messages, have definitions for "sexually explicit," "explicit sexual material," or "obscene."[22]

B. Labeling

A key feature of many state laws is the requirement that unsolicited commercial e-mail[23] (UCE) contain a label in the subject line of the message that identifies the mail as spam. Eighteen states require that subject lines of UCE begin with the characters "ADV:" and eighteen states require any UCE containing sexually explicit material or involving goods or services directed at individuals 18 years of age or older to be labeled "ADV:ADLT."[24] To avoid being over-inclusive, Kansas excludes from its "ADV:" labeling requirement any non-adult-oriented message sent to fewer than 500 recipients.[25] Despite these efforts, such requirements have proven relatively ineffective at prohibiting unidentified spam. In its recent report to Congress, the FTC noted that, despite being required by several states, only 2 percent of the spam it investigated contained "ADV:" on the subject line.[26]

C. Opt-Out

One of the perennial privacy battlefields is divided on opt-in versus opt-out standards. Under an opt-in standard, the sender of the commercial e-mail must obtain explicit permission from the potential recipient before sending the e-mail. California recently became the first state to approve an opt-in requirement for UCE.[27] Under the more business-friendly opt-out standard, an entity sending UCE must provide a valid link or e-mail address allowing the recipient to remove him or herself from the mailing list. Although 24 states require that UCE provide an opportunity for a recipient to opt-out of receiving any further e-mail, only 21 of these states actually require that spammers honor such requests.[28] While Minnesota, North Dakota, and Pennsylvania impose an additional requirement that recipients of UCE receive notice that they may opt-out, those statutes still fail to sanction a violation of

22. *See infra* app. 1.

23. From this point on, unless otherwise noted, the term "unsolicited commercial e-mail" (UCE) refers generically to all the variations of this term used by the various states.

24. *See infra* app. 1.

25. KAN. STAT. ANN. § 50-6,107(c)(1)(C) (Supp. 2002).

26. *See* Prepared Statement, *supra* note 6, at 4.

27. CAL. BUS. & PROF. CODE §§ 17529 to 17529.9, 17538.45 (West Supp. 2003).

28. *See infra* app. 1; *see also* statutes cited, *supra* note 15.

a recipient's request.[29] As mentioned above, the FTC study indicated that 63% of the opt-out links within the sampled e-mail failed to work.[30]

D. Reply Address

Twenty states require that UCE contain a valid and functioning reply e-mail address.[31] Of those states, ten permit the provision of a toll-free telephone number as an alternative opt-out method.[32]

E. Prohibited Behavior

State legislation most aggressively targets the use of falsified transmission or routing information. Many spammers engage in a number of deceptive sending techniques, including the unauthorized use of open relays and "spoofing."[33] By design, these activities mask the true source of the UCE. For example, messages are often sent through the servers of innocent third parties, known as open relays, in an attempt to disguise the true geographic and electronic origin of the messages, as well as avoid detection and interception by filter systems.[34] Through another technique known as "spoofing," spammers can fake the names and addresses contained in the "from" or "reply to" fields of an e-mail message header. On its face, the "spoofed" message appears to have come from a legitimate third party so as not to alert the recipient of the actual source.[35]

Thirty-two states currently prohibit such falsification of transmission or routing information in UCE.[36] Twenty-five states ban the use of a third-party's domain name or Internet address without that party's consent.[37] Additionally, twelve states forbid the sale or distribution of software that is ei-

29. *See* MINN. STAT. ANN. § 325F.694 (West Supp. 2004); N.D. CENT. CODE §§ 51-27-01 to -09 (2003); 18 PA. CONS. STAT. ANN. §§ 5903, 7661 (West Supp. 2003); 73 PA. CONS. STAT. ANN. § 2250 (West Supp. 2003).

30. Prepared Statement, *supra* note 6, at 3.

31. *See infra* app. 1.

32. *See infra* app. 1.

33. *See* CERT Coordination Center, *Spoofed/Forged Email*, *at* http://www.cert.org/tech_tips/email_spoofing.html (site updated Sept. 2, 2002; last visted Feb. 8, 2004); Open Relay Database, *Why do Open Relays Represent a Problem?*, *at* http://www.ordb.org/faq (last visited Feb. 8, 2004).

34. Open Relay Database, *Why do Open Relays Represent a Problem?*, *at http://www.ordb.org/faq* (last visited Feb. 8, 2004).

35. CERT Coordination Center, *Spoofed/Forged Email*, *at http://www.cert.org/tech_tips/email_spoofing.html*. (last visited Feb. 8, 2004).

36. *See infra* app. 1.

37. *See infra* app. 1.

ther primarily designed to facilitate or enable the falsification of transmission or routing information or that has limited use for any other function.[38]

False and misleading subject lines are an effective ploy used by spammers to entice a recipient to open and read a message that he or she might otherwise disregard. The FTC found that 22 percent of all the spam that it investigated, and over 33 percent of adult-oriented spam, contained false or misleading information in the subject line of the message.[39] Seventeen states prohibit the inclusion of false or misleading information in the subject line.[40]

California and Virginia, two states that aggressively prosecute spammers, ban the transmission of UCE in violation of the policies of an electronic mail service provider (EMSP).[41] Virginia-based AOL cited this provision in a number of recent lawsuits against large-scale spammers.[42]

F. Civil Actions

States differ on the issue of who may bring civil actions for spamming violations. Twenty-eight states permit both UCE recipients and Internet or e-mail service providers to bring civil suits to recover damages from spammers.[43] In contrast, Idaho and Nevada only permit suits by recipients,[44] while Pennsylvania only permits suits by service providers.[45] All thirty-one of these states allow the plaintiff to seek actual or statutory damages and all but four of them authorize recovery of costs and attorneys' fees.[46] Nine states allow for injunctions against further violations of the law.[47]

38. *See infra* app. 1.

39. Prepared Statement, *supra* note 6, at 4.

40. *See infra* app. 1.

41. CAL. BUS. & PROF. CODE §§ 17529 to 17529.9, 17538.45 (West Supp. 2003); VA. CODE ANN. § 18.2-152.12 (Michie Supp. 2003).

42. In April 2003, AOL commenced five separate actions in the Eastern District of Virginia against several named and anonymous spammers seeking damages and injunctive relief under the federal Computer Fraud & Abuse Act, the Virginia Computer Crimes Act, the Washington Commercial Electronic Mail Act, the Washington Consumer Protection Act, and the common law. America Online Inc. v. Byte Night LLC, No. 03-465-A (E.D. Va. April 11, 2003); America Online Inc. v. Maryland Internet Marketing Inc., No. 03-469-A (E.D. Va. April 14, 2003); America Online Inc. v. Doe, No. 03-472-A (E.D. Va. April 14, 2003); America Online Inc. v. Doe, No. 03-473-A (E.D. Va. April 14, 2003); America Online Inc. v. Doe, No. 03-474-A (E.D. Va. April 14, 2003).

43. *See infra* app. 1.

44. IDAHO CODE § 48-603E (2000); NEV. REV. STAT. ANN. 41.730-.735 (Michie 2002).

45. 73 PA. CONS. STAT. ANN. § 2250.8 (West Supp. 2003).

46. *See infra* app. 1.

47. *See infra* app. 1.

Statutory damage provisions vary greatly from state to state. Many states set an amount of $10 per violation with the total fine not to exceed up to $25,000 per day, while other states' fines are as high as $500 or $1,000 per violation.[48] In some states, the fines for recipients and providers differ—the fine for recipients is set higher in some states while the fine for providers is higher in others.[49] Maine provides for treble damages for willful or knowing violations,[50] and South Dakota allows treble damages for willful, knowing, or repeated violations.[51] Michigan gives injured parties the right to recover statutory damages in civil actions against recipients or providers of up to $250,000 for each day that the violation occurs.[52]

G. Criminal Sanctions

Seven states provide for both misdemeanor and felony sanctions, while an additional ten states impose only misdemeanor penalties.[53] Virginia recently elevated violations involving a high volume of UCE to felony status.[54] Under Virginia law, it is now a felony for anyone to falsify or forge transmission or routing information, or to sell or distribute software primarily designed to facilitate or enable the falsification of such information if: (1) the volume of the UCE exceeded (a) 10,000 attempted recipients in any 24-hour period, (b) 100,000 attempted recipients in any 30-day period, or (c) 1 million attempted recipients in any one-year period; *or* (2) the revenue generated from a specific UCE exceeded $1,000 or the total revenue generated from all UCE to any EMSP exceeded $50,000.[55]

H. Jurisdiction

States have been very careful in drafting their legislation in order to provide an appropriate jurisdictional basis and to avoid potential problems with the dormant Commerce Clause. The most popular approach is to provide jurisdiction if the recipient of the e-mail is within the state and the sender knew or had reason to know that the person resided in that state or had the means to ascertain that information.[56] Twenty-four states extend jurisdic-

48. *See infra* app. 1.

49. *See infra* app. 1.

50. 2003 Me. Laws 327.

51. S.D. CODIFIED LAWS § 37-24-40 (Michie 2003).

52. MICH. COMP. LAWS § 445.2508(b)(ii) (2003).

53. *See infra* app. 1 (felony and misdemeanor sanctions adopted in Ark., Conn., Mich., Nev., N.C., Pa. and Va.; misdemeanor sanctions adopted in Ariz., Cal., Del., Ill., Cal., La., Ohio, R.I., Tex., Utah and Wis.).

54. *See* VA. CODE ANN. § 18.2-152.3:1(B) (Michie Supp. 2003).

55. *Id.*

56. *See infra* app. 1.

tion if the recipient is within the state, twelve states extend jurisdiction if the message was sent from within the state, five states require that the e-mail be delivered to a resident of the state via equipment located within that state, three states require that a provider has equipment in the state, and two states require that there be "use" of a computer within the state.[57] Some states also extend jurisdiction for more than one of the above reasons.[58]

Two appellate decisions have already upheld the validity of state UCE laws. In *State v. Heckel*, the Supreme Court of Washington upheld the validity of that state's UCE law.[59] The Attorney General of Washington filed suit against an Oregon resident, alleging: (1) the use of false or misleading information in the subject lines of UCE; (2) misrepresentation of transmission path information and the routing of UCE through at least a dozen domain names without permission; and (3) failure to include a valid return e-mail address to which recipients could respond.[60] The state sought an injunction and civil penalties along with costs and attorneys' fees, but the trial court found for the defendant, holding that the state law violated the Commerce Clause.[61]

The Supreme Court of Washington, applying the two-prong test established by the United States Supreme Court in *Pike v. Bruce Church, Inc.*,[62] upheld the state law. The Court found that the law was facially neutral—it did not discriminate against interstate commerce in favor of intrastate economic interests.[63] The court stated that:

> [The] Act reaches only those deceptive UCE messages directed to a Washington resident or initiated from a computer located in Washington; in other words, the Act does not impose liability for messages that are merely routed through Washington or that are read by a Washington resident who was not the actual addressee.[64]

In so holding, the court found that the local benefits of the law outweighed any alleged burden on interstate commerce.[65]

Similarly, in *Ferguson v. Friendfinders, Inc.*,[66] a California appellate court held that the state's UCE law did not violate the dormant Commerce

57. *See infra* app. 1.

58. *See infra* app. 1.

59. 24 P.3d 404, 412-13 (Wash. 2001).

60. *Id.* at 407.

61. *Id.*

62. 397 U.S. 137 (1970).

63. *Heckel*, 24 P.3d at 409.

64. *Id.* at 413.

65. *Id.* at 409.

66. 115 Cal. Rptr. 2d 258 (Cal. Ct. App. 2002).

Clause. In *Ferguson*, the plaintiff alleged that he had received unsolicited e-mail: (1) whose subject line did not begin with the characters "ADV:;" (2) that failed to contain information about how to opt-out from future e-mail; (3) that failed to contain a valid return e-mail address; and (4) whose headers were altered in order to mask the identity of the sender, all in violation of California's law.[67] Much like in *Heckel*, the court applied the *Pike* standard and upheld the law.[68] The appellate court noted that the statute applied only to "e-mail users who send UCE to California residents via equipment located in California."[69] Thus, the "Legislature ensured that the statute would not reach conduct occurring 'wholly' outside the State."[70] While jurisdictional challenges to other states' laws remain possible, *Ferguson* and *Heckel* provide strong support for the validity of such UCE laws.

III. Federal Legislation

Depsite several attempts, no spam-related bill had passed both houses prior to the 108th Session of Congress. During the 108th Session, a number of such proposals were pending before the House and the Senate. Table 2 of this article summarizes the proposed legislation.

A. The House

Three pieces of legislation were before the House during the 108th Session. The first, the REDUCE Spam Act of 2003,[71] was probably the most similar to many of the existing state laws. The bill required that UCE be clearly identified as such, possibly by the familiar "ADV:" and "ADV:ADLT" labels, that UCE contain notice of and honor opt-out requests, and that UCE contain a valid return e-mail address.[72] The bill prohibited falsification of header or routing information and false or misleading subject lines.[73] It also provided for a private right of action for recipients of UCE and for Internet access service providers, both of whom could seek actual or statutory damages, as well as costs and attorneys fees.[74] The bill did not, however, provide any criminal sanctions. It would have preempted any state law that pertained to any activity covered in its provisions.

The two other bills before the House were similar in structure, but contained some important differences. The Reduction in Distribution of Spam

67. *Id.* at 261.

68. *Id.* at 261-63.

69. *Id.* at 265.

70. *Id.*

71. REDUCE Spam Act of 2003, H.R. 1933, 108th Cong. (2003).

72. *Id.*

73. *Id.* at § 4(1).

74. *Id.*

Act of 2003[75] and the Anti-Spam Act of 2003[76] both required identification of a message as an advertisement, but without requiring use of the "ADV:" and "ADV:ADLT" labels. Both required notice of and adherence to opt-out requests, required the inclusion of the sender's physical street address, and prohibited falsified header information and the use of third party addresses or domain names.[77] Also, both bills established criminal sanctions for violations as well as providing for civil actions by EMSPs and state attorneys general, but, significantly, not by recipients of spam.[78]

Both bills prohibited the targeting of illegally harvested e-mail addresses using automated means, but the Anti-Spam Act of 2003 also prohibits dictionary attacks of commercial e-mail.[79] Furthermore, the Anti-Spam Act also prohibited false or misleading subject lines and the failure to place warning labels on commercial e-mail containing sexually oriented material.[80] Possibly most significant, however, was the difference between the two bills' definitions of the term "commercial electronic mail message." The Reduction in Distribution of Spam Act of 2003 only included those messages whose "primary purpose" was the commercial advertisement or promotion of a product or service, while the Anti-Spam Act of 2003 included all messages that "contained" a commercial advertisement or promotion of a product or service.[81]

B. The Senate

Of the five major bills before the Senate, two were similar to existing state laws and the bills before the House. The CAN-SPAM Act of 2003[82] and the Stop Pornography and Abusive Marketing (SPAM) Act of 2003[83] both required identification of UCE as advertisement, although only the latter specifically required the "ADV" label. Both required UCE to contain notice of and honor requests to opt-out of further messages[84] and also required the

75. Reduction in Distribution of Spam Act of 2003, H.R. 2214, 108th Cong. (2003).

76. Anti-Spam Act of 2003, H.R. 2515, 108th Cong. (2003).

77. H.R. 2214 § 101; H.R. 2515 § 101.

78. H.R. 2214 § 102; H.R. 2515 § 102.

79. H.R. 2515 § 102 ("The Anti-Spam Act of 2003 describes a dictionary attack as when an e-mail address is generated "by use of automated means based on permutations of combining names, letters, or numbers for the purpose of sending commercial electronic mail.")

80. *Id*.

81. H.R. 2214 § 304; H.R. 2515 § 304.

82. CAN-SPAM Act of 2003, S. 877, 108th Cong. § 5(5)(a) (2003).

83. Stop Pornography and Abusive Marketing (SPAM) Act of 2003, S. 1231, 108th Cong. § 201(b) (2003).

84. S. 877 § 5(a)(5)(B); S. 1231 § 204(a)(2).

inclusion of the sender's physical street address.[85] Both bills prohibited falsified header information and false or misleading subject lines.[86] Only the proposed SPAM Act prohibited UCE that violates the policies of the EMSP.[87] With respect to remedies, both provided for civil actions by EMSPs[88] and state attorneys general,[89] but only the SPAM Act provided for a right of action by recipients.[90] Unlike the SPAM Act, the CAN-SPAM Act provided for misdemeanor criminal sanctions,[91] but the former called for the creation of a national "No-Spam Registry."[92]

The three other bills before Senate during the 108th Session took varied approaches to the problem of spam. The Computer Owners' Bill of Rights[93] sought to establish a registry for those who did not wish to receive any spam.[94] The Ban on Deceptive Bulk E-Mail Act of 2003 criminalized: (1) the falsification of e-mail transmission, routing and subject line information; (2) the transmission of e-mail to anyone who requests not to receive it; and (3) the collection of e-mail addresses from public and private spaces for the purpose of transmitting UBCE.[95] Significantly, it also deemed such violations to be predicate offenses for purposes of the Racketeering Influenced and Corrupt Organization Act.[96] The Criminal Spam Act of 2003 criminalized deceptive transmissions of multiple commercial e-mail messages and the falsification of header information in multiple commercial e-mail messages.[97] The severity of the offense was to be based partially on the volume of the messages sent.[98]

85. S. 877 § 5(a)(5)(C); S. 1231 § 206.

86. S. 877 § 5(a)(1)-(2); S. 1231 § 203.

87. S. 1231 § 202.

88. S. 877 § 6; S. 1231 § 304(a).

89. S. 877; S. 1231 § 303.

90. S. 1231 § 305.

91. S. 877 § 4

92. S. 1231 § 101.

93. Computer Owners' Bill of Rights, S. 563, 108th Cong. (2003).

94. S. 563 § 5(a).

95. Ban on Deceptive Bulk E-Mail Act of 2003, S. 1052, 108th Cong. (2003).

96. S. 1052 § 2(b)(1).

97. Criminal Spam Act of 2003, S. 1293, 108th Cong. (2003).

98. Under Senate bill 1293, punishment for not more than three years is authorized for offenses involving a volume of e-mail exceeding 2,500 pieces within a 24-hour period, 25,000 pieces within a 30-day period, or 250,000 within a 1-year period. *Id.* at § 1037(b)(2)(B)-(C). This is similar to the approach taken by the new Virginia law, under which it is a felony to transmit UBE to more than 10,000 attempted recipients in any 24-hour period, 100,000 attempted recipi-

C. Congress Passes the CAN-SPAM Act of 2003

Before leaving the Senate, several amendments were made to the CAN-SPAM Act. Most of the changes came from provisions contained in the Spam Act of 2003 and the Criminal Spam Act of 2003. The felony and misdemeanor sanctions proposed in the Criminal Spam Act of 2003, including the provisions that determined the severity of the offense based upon the volume of the UCE, were incorporated into the approved CAN-SPAM Act.[99]

Several provisions from the Spam Act of 2003 were included in the enacted legislation, although without specific requirements and with varying timetables. First, while stopping short of the mandatory establishment of a National No-Spam Registry, as proposed in the Spam Act of 2003, the enacted legislation requires the FTC to report back to Congress within 6 months of enactment with a plan for establishing a nationwide Do-Not-E-Mail registry.[100] The FTC has the discretion to implement such a plan no sooner than 9 months after enactment.[101]

Secondly, while the enacted legislation does not provide for a right of private civil action, as was proposed by the Spam Act of 2003, it does require the FTC to report back to Congress within 9 months with a plan to reward those individuals who supply information about violations of the law.[102] The system would grant a reward of at least 20 percent of the total civil penalty collected.[103]

Finally, while not requiring the inclusion of the "ADV:" label in the subject line of unsolicited commercial e-mail, as proposed by the Spam Act of 2003, as well as several other existing state laws, the enacted legislation requires the FTC to report back to Congress within 18 months with a plan for improving identification of such e-mail.[104] The plan could eventually require the use of the "ADV" label in the subject line of commercial e-mail.[105]

---

ents in any 30-day period, or one million attempted recipients in any 1-year period. VA. CODE ANN. § 18.2-152.3:1(B) (Michie Supp. 2003).

99. 108 Pub. L. No. 187, § 4, 117 Stat. 2699, 2703 (2003) (to be codified at 15 U.S.C. § 7703).

100. 108 Pub. L. No. 187, § 9, 117 Stat. 2699, 2716 (2003) (to be codified at 15 U.S.C. § 7708(a)).

101. *Id.* (to be codified at 15 U.S.C. § 7708(b)).

102. 108 Pub. L. No. 187, § 11, 117 Stat. 2699, 2717 (2003) (to be codified at 15 U.S.C. § 7710(1)).

103. *Id.* (to be codified at 15 U.S.C. § 7710(1)(a)).

104. *Id.* (to be codified at 15 U.S.C. § 7710(2)).

105. *Id.*

D. Preemption of State Laws

One of the most significant and controversial provisions of the CAN-SPAM Act of 2003 mandates the preemption of state law. It specifically preempts any state law that "expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message."[106] It exempts from preemption any state laws that "are not specific to electronic mail, including State trespass, contract or tort law"[107] and other state laws "to the extent that those laws relate to acts of fraud or computer crime."[108]

The CAN-SPAM Act preempts many of the state laws discussed in the first part of this article. Unless the law particularly relates to fraud, it will likely be preempted. For example, California recently passed a law that was to take effect on January 1, 2004, which would have instituted an "opt-in" system, effectively banning UCE.[109] However, this law was preempted.[110] New York has never passed a specific spam statute. Rather, its Attorney General has fairly aggressively pursued spammers using traditional business and fraud statutes.[111] States will probably have to follow this approach in their pursuit of spammers. Non-spam laws that relate to acts of fraud are expressly *not* preempted by the new federal legislation.[112]

Prior to the passage of the CAN-SPAM Act, at a *Spam Forum* held by the FTC in April-May 2003, a group of 44 attorneys general announced that they would not support the proposed CAN-SPAM Act of 2003 because it believed that the bill would preempt existing state laws that, in many states, provided for stronger protection against spam.[113] Subsequently, the National Association of Attorneys General warned Congress that "[t]he bill creates so many loopholes, exceptions, and high standards of proof, that it provides minimal consumer protections and creates too many burdens for effective

106. 108 Pub. L. No. 187, § 8, 117 Stat. 2699, 2716 (2003) (to be codified at 15 U.S.C. § 7707(b)(1)).

107. *Id*. (to be codified at 15 U.S.C. § 7707(b)(2)(A)).

108. *Id*. (to be codified at 15 U.S.C. § 7707(b)(2)(B)).

109. 2003 Cal. Adv. Legis. Serv. 487 (Deering).

110. *See* Stefanie Olsen, *California 'Disempowered' By Federal Spam*, CNET News.com, January 22, 2004, *available at* http://news.com.com/2100-1028-5145849.html (last visited Feb. 8, 2004).

111. *See* Saul Hansell, *New York and Microsoft Expected to File Civil Suits in Spam Case*, N.Y. TIMES, December 18, 2003, at C1.

112. 108 Pub. L. No. 187, § 8, 117 Stat. 2699, 2716 (2003) (to be codified at 15 U.S.C. § 7707(b)(2)(B)).

113. *See* David McGuire, *States Object to Spam Legislation*, WASH. POST, April 30, 2003, *available at* http:/www.washingtonpost.com/ac2/wp-dyn/A60659-2003Apr30.html (last visited Feb. 8, 2004).

enforcement."[114] Furthermore, the chairman of the FTC was not in favor of passage of the bill and predicted that, after passage, the FTC would continue to use pre-existing laws to prosecute spammers.[115]

IV. CONCLUSION

The passage of a federal spam law was long anticipated. A strong federal law would have provided a much-needed uniform approach to curtailing the abuses of spam. It appears, however, that the CAN-SPAM Act of 2003 will not only fail to stem the tide of UCE, but will also derail some important state efforts to deal with the problem. The federal law lacks the strength to reduce the flow of UCE. States that have aggressively fought spam will have to rely on non-spam related laws to continue those battles. The best hope for the new federal law lies in the reports to be made by the FTC to Congress regarding additional plans to fight spam. Hopefully, those plans will provide the support necessary to effectively can spam.

114. *See* Declan McCollagh, *Bush OKs Spam Bill – But Critics Not Convinced*, CNET News.com, December 16, 2003, *available at* http://news.com.com/2100-1028-5124724.html (last visited Feb. 8, 2004).

115. *Id.*

APPENDIX 1. STATE SPAM LAWS

	Definitions for: **S**exually explicit or **O**bscene **U**nsolicited [commercial] [e-mail] **C**ommercial [e-mail] **B**ulk [e-mail] **E**-mail	Label ADV:	Label ADV:ADLT	Must contain opt-out	Must honor opt-out	Must include sender's e-mail or reply address	Must not contain falsified routing information	Must not contain false or misleading subject line	Prohibits use of third party address or domain name	Prohibits distribution of software to falsify routing information	Prohibits sending e-mail in violation of provider policy	Damages: Actual damages (for Recipient or Provider)	Damages: Statutory damages (each occurrence/maximum) (for Recipient or Provider)	Damages: Costs and attorneys' fees	Can seek injunction	Criminal sanctions (Misdemeanor/Felony)	Addresses preemption	Jurisdiction: Sent from within state	Jurisdiction: Provider has equipment in state	Jurisdiction: Recipient in state (or reasonable belief)	Jurisdiction: Delivered to resident by equipment in state
Alaska	SUC	√												√		M		√		√	
Arizona	UCE	√		√	√		√	√	√			RP	$10/25K	√		M		√	√	√	
Arkansas	SUCE		√	√	√	√	√	√	√	√		RP	10/25K	√		MF					
California	UCE			√[1]		T[2]	√	√	√		√	RP	1000/1M;P50/25K	√		M	√	√		√	√
Colorado	UE	√		√	√	√	√		√			RP	10	√							√
Connecticut	"UBE"[3]				√	√	√			√	√	RP	10/25K	√		MF			U[4]		
Delaware	CE "UBCE"			√	√	√				√						M				√	
Idaho	B			√	√	√	√	√	√			R	100/1000							√	
Illinois	UE	√	√	√	√	T	√	√	√	√		RP	10/25K	√		M					√
Indiana	CE "UCE"	√	√	√	√		√	√	√			RP	500	√	√			√		√	
Iowa	E "BE" "UBE"			√	√	√	√		√			RP	10/R500;P25K	√	√				√		
Kansas	C	√[5]	√	√	√	T	√	√	√	√		RP	500/10K	√	√			√		√	
Louisiana	SU[6]		√				√			√	√					M					
Maine	U'E	√	√	√	√	√	√		√			RP	R250;P1000(x3)	√	√					√	
Maryland	C	√		√			√	√	√			RP	R500;P1000	√				√		√	
Michigan	UC	√		√	√	T	√		√	√		RP	500/250K	√		MF		√		√	

[1] California requires opt-out for commercial e-mail provided for a preexisting or current business relationship; otherwise, opt-in is required for unsolicited commercial e-mail.

[2] T indicates that either a reply address or toll-free telephone number is required. In California, this is required only for commercial e-mail provided for a preexisting or current relationship.

[3] Quotation marks mean that the term is used without definition.

[4] U indicates a requirement that a person "use" a computer within the state.

[5] The "ADV:" label is not required if message is sent to fewer than 500 recipients per month.

[6] "Unsolicited bulk electronic mail" requires the same or similar message sent to more than 1000 recipients.

[7] "Unsolicited commercial e-mail" requires that the e-mail be sent to 2 or more recipients in the state.

Minnesota	C	√	√	√		T	√	√	√			RP	10-25/25-35K	√			√									√
Missouri	UC	√	√	√	√	T		√				RP	R500;P1000		√									√		
Nevada	E	√		√	√	√	√	√		√		R	50-500	√	√	MF								√		
New Mexico	U	√	√	√	√	T						RP	R25;P10/5K	√										√		
North Carolina	UC						√					RP	10/25K	√		MF								√		
North Dakota	C	√	√	√		T	√	√	√			RP	R500;P1000				√							√		
Ohio	E			√	√	√	√		√		√	RP	R100;P50/50K	√	√	M										
Oklahoma	UCE	√	√	√	√		√	√	√			RP	10/25K	√						√						
Oregon	UCE	√					√	√	√			RP	R200,500/25K;P1 000/25K	√										√		
Pennsylvania	SCE		√	√		√	√	√	√	√		P	1-10+	√		MF								√		
Rhode Island	"UBE"			√	√	T	√		√			RP	500/25K	√		M		√						√		
South Dakota	C	√	√				√	√	√			RP	500/10K(x3)	√	√					√				√		
Tennessee	"UBE"	√	√	√	√	T	√			√		RP	10/5K	√	√			√								√
Texas	OUCE	√	√	√	√	√	√	√	√			RP	10/25K	√		M										
Utah	SUCE	√	√	√	√	T	√		√			RP	10/25K	√		M		√		√				√		
Virginia	"UBE"						√			√	√	RP	R10;P1/25K	√		MF					U					
Washington	C						√	√	√			RP	R500;P1000					√						√		
West Virginia	SB					√	√	√	√	√		RP	R1000;P10/25K	√				√						√		
Wisconsin	OE		√													M								√		
Wyoming	C						√	√	√									√						√		

APPENDIX 2. PROPOSED FEDERAL SPAM BILLS

	Definitions for: **U**nsolicited [commercial] [e-mail] **C**ommercial [e-mail] **B**ulk [e-mail] **E**-mail **H**eader Information	Must include identification of message as advertisement	Label ADV:	Label ADV:ADLT	Must contain opt-out	Must honor opt-out	Must include sender's physical street address	Must not contain falsified header information	Must not contain false or misleading subject line	Prohibits use of third party address or domain name	Prohibits use of illegally harvested addresses	Prohibits sending e-mail in violation of provider policy	Damages: Actual damages (for **R**ecipient or **P**rovider or **S**tate Attorneys General)	Damages: Statutory damages (each occurrence/maximum) (for **R**ecipient or **P**rovider or **S**tate Attorneys General)	Damages: Costs and attorneys' fees	Can seek injunction	Prohibits class actions.	Criminal sanctions (**M**isdemeanor/**F**elony)	Addresses preemption
House																			
H.R. 1933	UCH	√	√	√	√	√	√[1]	√	√				RP	$10	√	√			√
H.R. 2214	UCEH	√			√	√	√	√		√	√		PS	P10/500K(x3) S100/1M(x3)	√	√	√	MF	√
H.R. 2515	CEH	√			√	√	√	√	√	√	√[2]		PS	P10/500K(x3)[3] P100[4] S500(X3)	√	√		MF	√
Senate																			
S. 563						√[5]													
S. 877[6]	UCEH	√			√	√	√	√	√	√	√		PS	P10/500K(x3)	√	√		M	√
S. 1052	E "UBCE"[7]				√	√		√			√[8]							F[9]	
S. 1231	UCH	√	√		√	√	√	√	√			√	RPS	R up to 1000 PS up to 10	√	√	√		
S. 1293	CH							√					PS	2-8/25K		√		MF	

[1] The e-mail must contain a valid sender-operated return e-mail address, rather than a physical street address.
[2] Also prohibits the use of dictionary attacks.
[3] For violations regarding inclusion and opt-out provisions.
[4] For violations regarding header information, subject headings, harvesting, dictionary attacks, and sexually oriented materials.
[5] Establishes a registry of e-mail addresses to which unsolicited marketing e-mails may not be sent.
[6] As originally proposed in April 2003.
[7] Quotation marks mean that the term is used without definition.
[8] Prohibits collection of e-mail addresses from public or private spaces for the purpose of transmitting "UBCE."
[9] Violations shall be considered predicate offenses for purposes of applying the Racketeering Influenced and Corrupt Organization Act.